



Print Server

PS Series



User Manual
Windows

Manufacturer:
SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany
Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: <http://www.seh.de>



Document:
Type: User Manual
Title: Print Server PS Series Windows
Version: 2.0

Online Links to Important Websites:

Free Guarantee Extension: <http://www.seh-technology.com/guarantee>
Support Contacts & Information: <http://www.seh-technology.com/support>
Sales Contacts & Information: <http://www.seh-technology.com/sales>
Downloads: <http://www.seh-technology.com/services/downloads.html>

InterCon is a registered trademark of SEH Computertechnik GmbH.

SEH Computertechnik GmbH has endeavored to ensure that the information in this documentation is correct. If you detect any inaccuracies please inform us at the address indicated above. SEH Computertechnik GmbH will not accept any liability for any error or omission. The information in this manual is subject to change without notification.

All rights are reserved. Copying, other reproduction, or translation without the prior written consent from SEH Computertechnik GmbH is prohibited.

© 2015 SEH Computertechnik GmbH

All trademarks, registered trademarks, logos and product names are property of their respective owners.

Contents

1	General Information	1
1.1	Your Print Server	1
1.2	Documentation	2
1.3	Support and Service	4
1.4	Your Safety	5
1.5	First Steps	6
1.6	Finding the Print Server (Determining the IP Address)	6
2	Printing in Windows	8
2.1	How to Set Up Socket Printing	9
2.2	How to Set Up LPD/LPR Printing	11
2.3	How to Set Up IPP Printing	14
2.4	How to Configure Encrypted Printing	16
3	Administration Methods	20
3.1	Administration via Print Server Homepage	21
3.2	Administration Via InterCon-NetTool	23
3.3	Administration via FTP/FTPS Connection	25
3.4	Administration via Email	27
4	Network Settings	31
4.1	How to Configure IPv4 Parameters	31
4.2	How to Configure IPv6 Parameters	34
4.3	How to Adapt the Network Speed	37
4.4	How to Configure NetBIOS/WINS	38
4.5	How to Configure the DNS	40
4.6	How to Configure Bonjour	41
4.7	How to Use SNMP	43
4.8	How to Configure POP3 and SMTP	43
4.9	How to Configure WLAN	47
5	Port Settings	51
5.1	How to Enable PJJ	51
5.2	How to Enable 1284.4/MLC	52
5.3	How to Define the Communication Mode	54

5.4	How to Configure COM1 Port Settings	55
6	Device Settings	57
6.1	How to Configure the Language of the Device	57
6.2	How to Configure the Device Time	58
6.3	How to Determine a Description.....	60
7	Print Server Status Information	61
7.1	How to View Status Information	61
7.2	What Status Information is Shown?	62
7.3	How to Print a Status or Service Page	64
8	Print Jobs and Print Data	68
8.1	How to Define a Timeout for Taking on Print Jobs	68
8.2	How to Assign Print Jobs Directly	69
8.3	How to Modify Print Data	71
8.4	How to Convert Print Data	72
8.5	How to Use Logical Printers (Filter Functions)	73
9	Printer Status and Printer Messages	78
9.1	How to View the Printer Status	78
9.2	How to Get Additional Printer Information	80
9.3	How to Get Printer Messages via Email.....	81
9.4	How to Get Printer Messages via SNMP Trap	83
9.5	How to View the Job History.....	85
10	Security	87
10.1	How to Define a Password for the Print Server (Read/Write Protection)	88
10.2	How to Disable the HTTP Access (Protection against Viruses)	89
10.3	How to Protect Printers against Unauthorized Access (IP Sender Control)	90
11	Certificate Management	93
11.1	How to View Certificates	94
11.2	How to Create a Self-Signed Certificate	96
11.3	How to Create a Certificate Request for a Requested Certificate... ..	98

11.4	How to Save a Requested Certificate in the Print Server.....	100
11.5	How to Save a PKCS12 Certificate in the Print Server.....	102
11.6	How to Save CA Certificates in the Print Server.....	103
11.7	How to Delete Certificates.....	104
12	Network Authentication	107
12.1	How to Configure EAP-MD5	108
12.2	How to Configure EAP-TLS	109
12.3	How to Configure EAP-TTLS	111
12.4	How to Configure PEAP	113
12.5	How to Configure EAP-FAST.....	115
13	Maintenance	118
13.1	How to Secure the Print Server Parameters (Backup)	119
13.2	How to Reset Parameters to their Default Values	123
13.3	How to Perform an Update	127
13.4	How to Restart the Print Server	133
14	Additional Feature – ThinPrint®.....	135
14.1	How to Address the Print Server in a ThinPrint Environment.....	136
14.2	How to Define the ThinPrint Port	136
14.3	How to Define the Bandwidth	137
14.4	How to Use ThinPrint AutoConnect.....	138
14.5	How Does the Print Server Receive Encrypted Data?.....	140
15	Additional Feature – Internet Protocol Security (IPsec) ..	141
15.1	How to Create IPsec Rules	145
15.2	How to Use IPsec Configuration Files	155
15.3	How to Define Exceptions	157
15.4	How to Enable IPsec Policies.....	157
16	Appendix.....	159
16.1	Glossary	159
16.2	Parameter List	162
16.3	Troubleshooting.....	193
16.4	List of Figures.....	197
16.5	Index	198

1 General Information



This chapter contains information concerning the device and the documentation as well as notes about your safety. You will learn how to benefit from your print server and how to operate the device properly.

What Information Do You Need?

- 'Your Print Server' ⇨ 1
- 'Documentation' ⇨ 2
- 'Support and Service' ⇨ 4
- 'Your Safety' ⇨ 5
- 'First Steps' ⇨ 6
- 'Finding the Print Server (Determining the IP Address)' ⇨ 6

Purpose

Print servers are active network components that receive print jobs from connected users or user groups within a network and forward them to printers or other end devices.

Supported Systems

Print servers have been designed for the use in the following systems:

- Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10
- Mac OS X 10.8.x, Mac OS X 10.9.x, Mac OS X 10.10.x

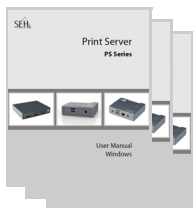


This document describes the usage in Windows environments. Information about the usage in other environments can be found in the relevant system-specific User Manual. For further information; see: 'Documentation' ⇨ 2.

Structure of the Documentation

1.2 Documentation

The print server documentation consists of the following documents:



User Manual

Detailed description of the print server installation, configuration, and administration. System-specific instructions for the following systems:

- Windows
- Mac



Quick Installation Guide

Information about security, hardware installation, and the initial operation procedure.

Scope and Content

This documentation describes a variety of print server models. This means that features will be described that may not be applicable to your print server. Information about the features of your print server can be found in the data sheet of your print server model.

Due to the multitude of supported operating systems, instructions are described exemplarily. The respective concept can be transferred to other versions of the operating system.

Document Features

This documentation has been designed as an electronic document for screen use. Many programs (e.g. Adobe® Reader®) offer a bookmark navigation feature that allows you to view the entire document structure.

This document contains hyperlinks to the associated information units. If you want to print this documentation, we recommend using the printer setting 'Duplex' or 'Booklet'.







Terminology Used in this Document

The explanation of technical terms used in this document is summarized in a glossary. The glossary provides a quick overview of technical matters and background information; see: ⇨ 159.

Symbols and Conventions

A variety of symbols are used within this document. Their meaning is listed in the following table:

Table 1: Conventions within the documentation

Symbol / Convention	Description
 Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
 Note	A notice contains information that should be heeded.
 Proceed as follows: 1. <i>Select...</i>	The 'hand' symbol marks the beginning of instructions. Individual instructions are set in italics.
 Confirmation	The arrow confirms the consequence of an action.
<input checked="" type="checkbox"/> Requirements	Hooks mark requirements that must be met before you can begin the action.
<input type="checkbox"/> Option	A square marks procedures and options that you can choose.
•	Eye-catchers mark lists.
	This sign indicates the summary of a chapter.
	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
Courier	Command lines are set in 'Courier' font.
'Proper names'	Proper names are put in inverted commas.

Support

1.3 Support and Service

SEH Computertechnik GmbH offers extensive Support. If you have any questions, please contact our hotline.



Monday – Thursday
Friday

8:00 a.m. – 4:45 p.m.
8:00 a.m. – 15:15 p.m.



+49 (0)521 94226-44



support@seh.de



<http://www.seh.de/>

Downloads

Downloads can be found on the SEH Computertechnik GmbH home-page:

<http://www.seh-technology.com/services/downloads.html>



For print servers you will find:

- current firmware/software
- current tools
- current documentation
- current product information
- product data sheets
- and much more

1.4 Your Safety

Read and observe all safety regulations and warnings found in the documentation, on the device and on the packaging. This will avoid potential misuse and prevent damages to people and devices.

SEH Computertechnik GmbH will not accept any liability for personal injuries, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings. SEH Computertechnik GmbH will not accept any liability for loss of data, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings.

Intended Use

Print servers are network interfaces for printers. They are designed for the direct integration of printers into networks. The print server has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the print server functionalities described in the documentation are regarded as improper uses. It is not allowed to make modifications to the hardware and software or to try to repair the device.

Safety Regulations

Before starting the initial operation procedure of the print server, please note the safety regulations in the 'Quick Installation Guide'. This document is enclosed in the packaging in printed form.

Warnings


Read and observe all warnings mentioned in this document. Warnings are found before any instructions known to be dangerous. They are presented as follows:




Warning!

1.5 First Steps

This section provides all the information that you need for a fast operational readiness.

 Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices; see: [⇒ 5](#).*
 2. *Carry out the hardware installation. The hardware installation comprises the connection of the ISD to the network and the mains supply; see: 'Quick Installation Guide'.*
 3. *Make sure that the print server has an IP configuration which is suitable for your network; see: [⇒ 6](#).*
 4. *Configure your clients for printing via the print server, see: [⇒ 9](#).*
-  Via the print server you can print to the printers connected.

1.6 Finding the Print Server (Determining the IP Address)

Why IP Addresses?

An IP address is used to address network devices in an IP network. TCP/IP network protocols require the storing of the IP configuration in the print server so that the device can be addressed within the network.

How Does the Print Server Obtain Its IP Configuration?


SEH print servers are shipped without IP configuration. Once the print server is connected to the network, it automatically receives an IP configuration via the boot protocols BOOTP or DHCP. If this is not the case, the print servers seeks a ZeroConf IP address from the ZeroConf address range (169.254.0.0/16).

How to Find The Print Server in the Network (Determining the IP Address)

The InterCon-NetTool is a software tool developed by SEH Computertechnik GmbH for the administration of SEH print servers. By means of this tool you can find the print server's IP address, as described below.



The client, printer and print server must be assigned to the same local network segment for the initial configuration.

 Proceed as follows:

1. Download the installation file for the InterCon-NetTool from the homepage of the SEH Computertechnik GmbH:
<http://www.seh-technology.com/services/downloads.html>



2. Start the installation file.
 3. Select the desired language.
 4. Follow the installation routine.
The InterCon-NetTool will be installed on your client.
 5. Start the InterCon-NetTool on your client.
- ↳ The InterCon-NetTool searches the network for existing print servers and displays them in the 'device list'.

If the print server has received an IP configuration via the boot protocols BOOTP or DHCP, you can identify it with the help of its type designation. If you are using several print servers of the same type, identify the print server using its hardware address. You can find the hardware address in the type plate at the bottom of the print server.

If the print server has assigned itself an IP address via ZeroConf from the address range (169.254.0.0/16) which is reserved for ZeroConf, it will be displayed in the device list under the 'ZeroConf' filter. Assign a new IP configuration to the print server, see below.



For more information on the InterCon-NetTool, see: 'Administration via InterCon-NetTool' ⇒ 15.

How to Change the IP Configuration of the Print Server

You can change the IP configuration later on.

- 'How to Configure IPv4 Parameters' ⇒ 31
- 'How to Configure IPv6 Parameters' ⇒ 34

2 Printing in Windows



This chapter describes printing via the print server in Windows.

The print server embeds non-network-ready printers into the network. In order to print via the print server, the printers connected to the print server must be set up as printers on the client system. This is done via the Windows settings.



The following descriptions show how printers are set up in Windows 10. The menu navigation in other Windows systems may vary. For more information, please read the printer setup instructions in your Windows user manual.

What Information Do You Need?

- 'How to Set Up Socket Printing' ⇨ 9
- 'How to Set Up LPD/LPR Printing' ⇨ 11
- 'How to Set Up IPP Printing' ⇨ 14
- 'How to Configure Encrypted Printing' ⇨ 16

Procedure

2.1 How to Set Up Socket Printing


Socket printing is carried out by means of direct TCP/IP ports.

Follow these steps if you want to print:

- 'Setting up the Printer on the Client' ⇨ 9
- 'Configuring the Printer Port' ⇨ 10

Setting up the Printer on the Client

- The print server is connected to the network and the printer; see: Quick Installation Guide.
- The print server and the printer are turned on.
- The print server has a suitable IP configuration, see: ⇨ 7.
- You know the print server's current IP address; see: ⇨ 7.

 Proceed as follows:

1. *Open the Start menu.*
2. *Select Settings.*
The Settings dialog appears.
3. *Select Devices.*
The Add printers & scanners dialog appears.
4. *Select Add a printers or scanners.*
Printers and scanners are searched for.
5. *Scroll down to the end of the result list and select The printer that I want isn't listed.*
The Add printer dialog appears.
6. *Tick Add a local printer or network printer with manual settings.*
7. *Tick Create a new port.*
8. *From the list Type of port, select Standard TCP/IP Port.*
9. *Click Next.*
10. *In the Hostname or IP address box, enter the IP address of the print server.*




Omit leading zeros from the IP address!

11. *Enter a description into the Port name box.*
 12. *Untick Query the printer and automatically select the driver to use.*
 13. *Click Next.*
 14. *(In the area Device Type, tick Standard.)*
 15. *(Select Generic Network Card from the list.)*
 16. *(Click Next.)*
 17. *From the list Manufacturer and Printers, select the printer model.*
 18. *Click Next.*
 19. *Enter a description into the Printer name box.*
 20. *Click Next.*
The printer is being installed.
 21. *Tick Do not share this printer.*
 22. *Click Next.*
 23. *Click Print a test page.*
The test page is printed.
 24. *Click Finish.*
- ☞ *The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.*

Configuring the Printer Port

Via the printer port (9100 - 9107) different logical printers are addressed. The logical printer defines the printer port to which the print data is sent. This is relevant for print server models with several physical printer ports (COM1, USB1, etc.). For further information; see: ⇒ 68.

 Proceed as follows:

1. *In the taskbar, enter 'Devices and Printers' into the search box.*
The search results are displayed.
2. *In the search results, select Devices and Printers.*
The Devices and Printers dialog appears.
3. *In the list, select the printer.*

4. From the shortcut menu, select **Printer properties**.
The Properties dialog appears.
 5. Select the **Ports** tab.
 6. In the list, select the port.
 7. Click **Configure**.
The Configure Standard TCP/IP Port Monitor dialog appears.
 8. In the **Protocol** area, tick the option **Raw**.
 9. In the **Raw Settings** area, define the **Port Number**.
 10. **Untick** **SNMP Status Enabled**.
 11. Click **OK** to confirm.
- ↪ The settings will be saved.

2.2 How to Set Up LPD/LPR Printing

When using the printing protocol Line Printer Daemon/Line Printer Remote-Protokoll (LPD/LPR), printing is done via a TCP/IP connection.

Mode of Operation

LPD/LPR consists of two components:


- Line Printer Daemon (LPD) refers to the process which receives print jobs from the LPR client. LPD runs on the print server. Thus the print server is called LPD server.
- Line Printer Remote (LPR) is the term for the process which sends print jobs to a printer or respectively to a print queue. The client (PC, etc.) which sends the print job is the LPR client and must be equipped with the required software.


Procedure

Follow these steps if you want to print:

- 'Activating LPR on the Client' ⇨ 12.
- 'Setting up the Printer on the Client' ⇨ 12.
- 'Setting Up the Printer Port' ⇨ 13.


Requirements**Activating LPR on the Client**

 Proceed as follows:

1. *In the taskbar, enter 'Programs and Features' into the search box.
The search results are displayed.*
 2. *In the search results, select **Programs and Features**.
The **Programs and Features** dialog appears.*
 3. *Select **Turn Windows features on or off**.
The **Windows Features** dialog appears.*
 4. *Under **Print and Document Services** activate **LPR Port Monitor**.*
 5. *Click **OK** to confirm.*
-  LPR is activated on the client.

Setting up the Printer on the Client

- The print server is connected to the network and the printer; see: Quick Installation Guide.
- The print server and the printer are turned on.
- The print server has a suitable IP configuration, see: ⇨ 7.
- You know the print server's current IP address; see: ⇨ 7.

 Proceed as follows:

1. *Open the **Start** menu.*
2. *Select **Settings**.
The **Settings** dialog appears.*
3. *Select **Devices**.
The **Add printers & scanners** dialog appears.*
4. *Select **Add a printers or scanners**.
Printers and scanners are searched for.*
5. *Scroll down to the end of the result list and select **The printer that I want isn't listed**.
The **Add printer** dialog appears.*
6. *Tick **Create a new port**.*
7. *From the list **Type of port**, select **Standard TCP/IP Port**.*


8. *Into the **Address** box, enter the IP address of the print server.*



Omit leading zeros from the IP address!

9. *Enter a description into the **Port name** box.*
 10. *Untick **Query the printer and automatically select the driver to use**.*
 11. *Click **Next**.*
 12. *(In the area **Device Type**, tick **Standard**.)*
 13. *(Select **Generic Network Card** from the list.)*
 14. *(Click **Next**.)*
 15. *From the list **Manufacturer and Printers**, select the printer model.*
 16. *Click **Next**.*
 17. *Enter a description into the **Printer name** box.*
 18. *Click **Next**.*
The printer is being installed.
 19. *Click **Print a test page**.*
The test page is printed.
 20. *Click **Finish**.*
- ☞ *The printer is set up on the client. Set up the printer port for LPD/LPR printing ⇒ 13.*

Setting Up the Printer Port

 Proceed as follows:

1. *In the taskbar, enter 'Devices and Printers' into the search box.*
The search results are displayed.
2. *In the search results, select **Devices and Printers**.*
*The **Devices and Printers** dialog appears.*
3. *In the list, select the printer.*
4. *From the shortcut menu, select **Printer properties**.*
*The **Properties** dialog appears.*
5. *Select the **Ports** tab.*
6. *In the list, select the port.*

Requirements


7. **Click Configure.**
The Configure Standard TCP/IP Port Monitor dialog appears.
 8. *In the list, select the port.*
 9. **Click Configure.**
 10. *The Configure Standard TCP/IP Port Monitor dialog appears.*
 11. *In the Protocol area, tick the option LPR.*
 12. *Into the Queue Name box, enter a logical printer (lp1 - lp8).*
The logical printer defines the printer port to which the print data is sent. This is relevant for print server models with several physical printer ports (COM1, USB1, etc.). If no logical printer is defined, the logical printer no. 1 will be used automatically. For further information; see: ⇨ 68.
 13. **Untick SNMP Status Enabled.**
 14. **Click OK to confirm.**
- 👉 The settings will be saved. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

2.3 How to Set Up IPP Printing

In IPP (Internet Printing Protocol) the print data is transmitted via HTTP to the printer. When printing via IPP, the print server is addressed via a Uniform Resource Identifier (URI). The syntax of the URI looks as follows:

```
http://<IP address>:631/ipp/<logical printer>
```

- The print server is connected to the network and the printer; see: Quick Installation Guide.
- The print server and the printer are turned on.
- The print server has a suitable IP configuration, see: ⇨ 7.
- You know the print server's current IP address; see: ⇨ 7.

 Proceed as follows:

1. *Open the Start menu.*
2. **Select Settings.**
The Settings dialog appears.
3. **Select Devices.**
The Add printers & scanners dialog appears.

4. **Select Add a printers or scanners.**
Printers and scanners are searched for.
5. **Scroll down to the end of the result list and select The printer that I want isn't listed.**
The Add printer dialog appears.
6. **Tick Select a shared printer by name.**
7. **Into the Select a shared printer by name box, enter the print server's IP address and the socket number for IPP printing. If necessary, enter the name of the logical printer (lp1–lp8):**
`http://<IP address>:631/ipp/<logical printer>`
With print server models with several physical ports, the logical printer is also used to address the port. If no name or an incorrect name has been entered, the print data is automatically routed to the printer through logical printer no.1. For further information; see: ↗ 68.



Omit leading zeros from the IP address!

8. **Click Next.**
The Add Printer Wizard appears.
 9. **From the list Manufacturer and Printers, select the printer model.**
 10. **To confirm click OK.**
The printer is being installed.
 11. **Click Next.**
 12. **Print a test page.**
 13. **Click Finish.**
- ↗ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server.

2.4 How to Configure Encrypted Printing

You can encrypt the print data that is sent to the print server from the client.

Mode of Operation

The communication between client and print server is encrypted via SSL/TLS. In this process, the print server is addressed via a Uniform Resource Identifier (URI). The syntax of the URI looks as follows:

```
https://<IP address>:443/ipp/<logical printer>
```

For authentication a print server certificate is required. The 'Common name' box of the print server certificate must contain the print server's IP address.

Procedure

In order to encrypted printing, proceed as follows:

- Create a self-signed certificate in the print server. Into the 'Common name' box, enter the IP address of the print server. Omit leading zeros from the IP address. See: 'Wie erstelle ich ein selbstsigniertes Zertifikat?' ⇨ 92.
- Save the print server certificate on the client from which you want to print; see: ⇨ 16.
- On the client, create a printer for the printer connected to the print server; see: ⇨ 18.




You must observe the following instructions in the indicated order. If this procedure is not adhered to, the printer connected to the print server cannot be set up as printer on the client.

Saving the Print Server Certificate on the Client

The print server certificate can be saved on the client via the Internet Explorer.

Requirements

- You have administrative rights on the client.
- The Internet Explorer is installed on the client. (It is installed by default in Windows 10.)

 Proceed as follows:


1. *In the taskbar, enter 'Internet Explorer' into the search box. The search results are displayed.*
2. *In the search results, right click on Internet Explorer. The context menu appears.*
3. *Select **Run as administrator**. A security query appears.*
4. *Confirm the security query by clicking **Yes**. The Internet Explorer starts.*
5. *Open an encrypted connection to the print server: To do this, enter 'https://' and the IP address of the print server as the URL. Example: https://10.168.1.234
The following message appears: **There is a problem with this website's security certificate.***
6. *Click **Continue to this website (not recommended)**. The Print Server Homepage appears. The address bar is red and shows a certificate warning.*
7. *In the address bar, click **Certificate error**. The popup **Untrusted Certificate** appears.*
8. *Click **View certificates**. The **Certificate dialog** appears.*
9. *Click **Install Certificate**. The **Certificate Import Wizard** appears.*
10. *Select **Local Machine**.*
11. *Click **Next**.*
12. *Select **Place all certificates in the following store**.*
13. *Click **Browse**. The **Select Certificate Store dialog** appears.*
14. *From the list, select **Trusted Root Certification Authorities**.*
15. *Click **OK** to confirm.
In the **Select Certificate Store dialog**, the folder **Trusted Root Certification Authorities** is displayed in the **Certificate store box**.*
16. *Click **Next**.*
17. *Click **Finish**.
A success message appears.*

Requirements

18. Confirm the success notification by clicking **OK**.
 19. Close the certificate dialog by clicking **OK**.
- ✎ The print server certificate is installed on the client.

Setting up the Printer on the Client

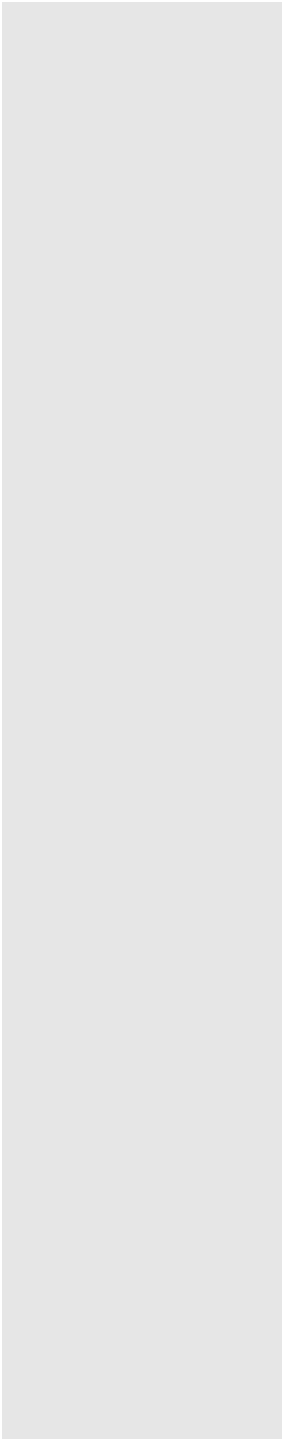
- The print server is connected to the network and the printer; see: Quick Installation Guide.
- The print server and the printer are turned on.
- The print server has a suitable IP configuration, see: ⇨ 7.
- You know the print server's current IP address; see: ⇨ 7.

 Proceed as follows:

1. *Open the Start menu.*
2. *Select Settings.*
The Settings dialog appears.
3. *Select Devices.*
The Add printers & scanners dialog appears.
4. *Select Add a printers or scanners.*
Printers and scanners are searched for.
5. *Scroll down to the end of the result list and select The printer that I want isn't listed.*
The Add printer dialog appears.
6. *Tick Select a shared printer by name.*
7. *Into the Select a shared printer by name box, enter the print server's IP address and the socket number for IPP printing. If necessary, enter the name of the logical printer (lp1–lp8):*
`https://<IP address>:443/ipp/<logical printer>`
With print server models with several physical ports, the logical printer is also used to address the port. If no name or an incorrect name has been entered, the print data is automatically routed to the printer through logical printer no.1. For further information; see: ⇨ 68.



In the URI, enter the IP address exactly as it is written in the file 'Common name' of the print server certificate. Omit leading zeros in both cases. Otherwise the print server cannot be addressed.

- 
8. *Click Next.*
The Add Printer Wizard appears.
 9. *From the list Manufacturer and Printers, select the printer model.*
 10. *To confirm click OK.*
The printer is being installed.
 11. *Click Next.*
 12. *Print a test page.*
 13. *Click Finish.*
- ↳ The printer is set up on the client. If you print via the printer you have set up, the print job will be printed on the printer connected to the print server. The print data is transmitted in an encrypted way.

3 Administration Methods



You can administer and configure the print server in a number of ways. The following chapter gives you an overview of the various administration options.

You will get information on when to use these methods and which functions these methods support.

What Information Do You Need?

- 'Administration via Print Server Homepage' ⇨ 21
- 'Administration Via InterCon-NetTool' ⇨ 23
- 'Administration via FTP/FTPS Connection' ⇨ 25
- 'Administration via Email' ⇨ 27

3.1 Administration via Print Server Homepage

Functionalities


The print server has a user interface, the Print Server Homepage, which can be opened in an Internet browser (Internet Explorer, Mozilla Firefox, Safari).

The print server can be configured and monitored via the Print Server-Homepage.

Requirements

- The print server is connected to the network, printer and the mains voltage.
- The print server has a suitable IP configuration, see: ⇨ 7.

Starting the Print Server Homepage


 Proceed as follows:

1. *Open your browser.*
 2. *Enter the IP address of the print server as the URL.*
- ⇨ The Print Server Homepage is displayed in the browser.



If the Print Server Homepage is not displayed, check the proxy settings of your browser.

You can also start the Print Server Homepage via the software tool 'InterCon-NetTool'.

 Proceed as follows:

1. *Select the print server in the device list.*
 2. *Select **Actions – Launch Browser** from the menu bar.*
- ⇨ The Print Server Homepage is displayed in the browser.

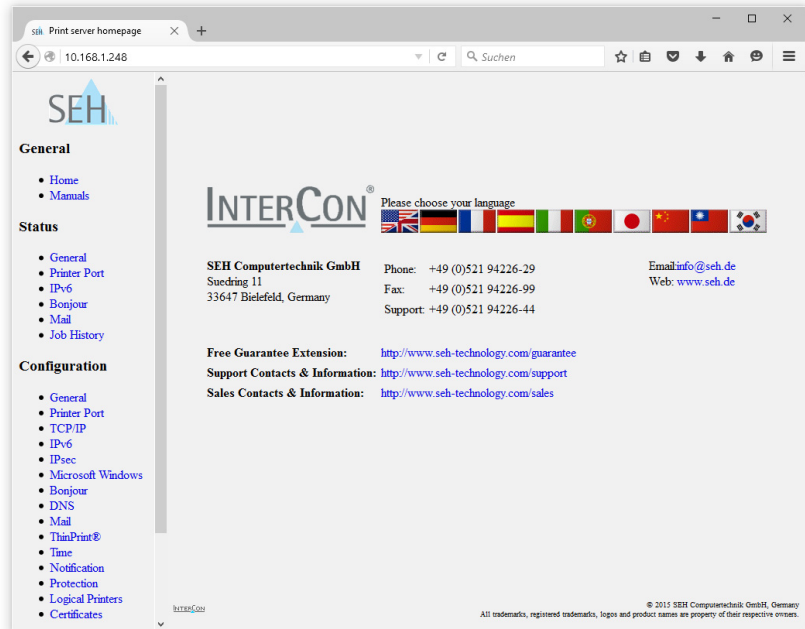


Fig. 1: Print server homepage - Home

Structure of the Print Server Homepage

The available menu items are located in the navigation bar (left hand). After selecting a menu item (simple mouse click), the corresponding page with its content is displayed.

You can set the language of the Print Server Homepage via **General – Home**. Simply select the relevant flag. You will also see the contact information of the manufacturer.

Clicking the **General – Manuals** link brings you to the SEH Computertechnik GmbH homepage. Here, you can download the latest manuals as *.pdf files.

All other menu items refer to the configuration of the print server and are described in this manual.



The appearance of the Print Server-Homepage depends on the print server model and software version.

3.2 Administration Via InterCon-NetTool

The InterCon-NetTool is a software tool developed by SEH Computertechnik GmbH for the administration of SEH print servers.


Mode of Operation

After the InterCon-NetTools is started, the network will be scanned for connected print servers. The network range to be scanned is freely definable. All print server found will be displayed in the 'device list'.

You can modify the device list and adapt it to your individual needs. You can select the print servers in the device list and configure them.


Installation

In order to use the InterCon-NetTool, the program must be installed on a computer with Windows operating system.


 Proceed as follows:

1. *Download the installation file for the InterCon-NetTool from the homepage of the SEH Computertechnik GmbH:*
<http://www.seh-technology.com/services/downloads.html>



2. *Start the installation file.*
 3. *Select the desired language.*
 4. *Follow the installation routine.*
-  The InterCon-NetTool will be installed on your client.

Program Start

You can identify the InterCon-NetTool by its icon: . The InterCon-NetTool can be started with the usual mechanisms of your operating system.

The program settings are saved in the 'InterCon-NetTool.ini' file. This file is stored in the user folder of the user that is currently logged in.

InterCon-NetTool Structure

After the program start you will see the main dialog with the following elements. The dialog may vary, depending on which elements you have chosen to be shown or hidden.

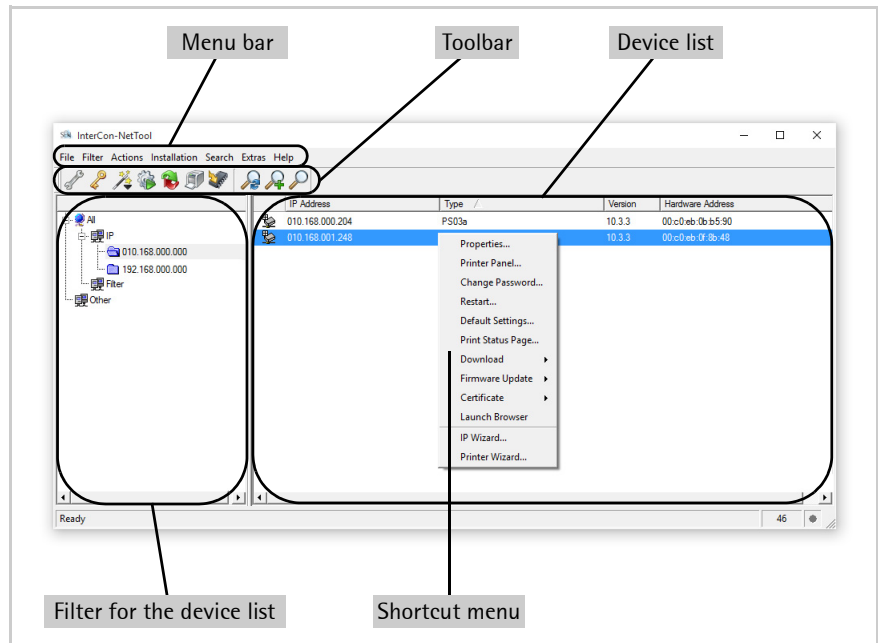


Fig. 2: InterCon-NetTool - Main dialog

Which Functions Are Supported?

The InterCon-NetTool allows you to

- 'assign an IPv4 configuration to the print server' ⇨ 7
- 'restart the print server' ⇨ 133
- 'reset the print server parameters to their default settings' ⇨ 122
- 'start the Print Server-Homepage' ⇨ 21
- 'carry out updates' ⇨ 133
- 'save and transfer the print server parameters' ⇨ 118
- 'switch from the BIOS mode to the default mode' ⇨ 195



Detailed information on how to use the InterCon-NetTool can be found in the Online Help. To start the Online Help, select **Help - Online Help** from the menu bar.

3.3 Administration via FTP/FTPS Connection

FTP

The File Transfer Protocol (FTP) allows the exchange of data between the print server and an FTP client in TCP/IP networks.


FTP over SSL/TLS (FTPS)

The print server also supports FTPS (FTP over SSL) for a safe data interchange between the print server and the client.

We recommend using SSL/TLS so that unencrypted user names, passwords, and data cannot be read by unauthorized persons.

Configuring Parameters via FTP Connection


You can configure all print server parameters via FTP. To this purpose, you must download the 'parameters' file to your local computer via FTP and then edit it.

 Proceed as follows:

1. *Change to the directory in which you wish to save the file.*
 2. *Open an FTP connection to the print server:*
Syntax: ftp <IP address>
Example: ftp 192.168.0.123
 3. *Enter an arbitrary user name.*
 4. *Enter the print server password or press the enter key if no password has been assigned.*
 5. *Transfer the 'parameters' file from the print server to your local computer:*

```
get parameters
```
 6. *Edit the file using a text editor.*
The syntax and values can be obtained from the parameter list; see: ⇨ [162](#).
 7. *Send the file back to the print server:*

```
put parameters
```
 8. *Close the FTP connection:*

```
quit
```
-  The print server will be configured using the new values.

Which Functions Are Supported?

An FTP/FTPS connection allows you to

- print a status page ⇒ 60
- print a service page ⇒ 61
- configure the printserver parameters ⇒ 25
- 'reset the print server parameters to their default settings' ⇒ 123
- 'query the printer status' ⇒ 76
- 'carry out updates' ⇒ 126

3.4 Administration via Email

You can administer the print server via email and thus via any computer with Internet access.

Functionalities

An email allows you to


- send print server information,
- print emails and attachments,
- perform an update on the print server or
- define print server parameters.

Requirements

- A DNS server has been configured on the print server, see: ⇒ [32](#).
- In order to receive emails, the print server must be set up as user with its own email address on a POP3 server.
- POP3 and SMTP parameters have been configured on the print server; see: ⇒ [36](#).

Sending Instructions via Email

If you want to administer the print server, you must enter the relevant instructions into the subject line of your email.

 Proceed as follows:

1. *Open an email program.*
2. *Write a new email.*
3. *Enter the print server address as recipient.*
4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction' ⇒ [27](#).*

5. *Send the email.*

👉 The print server receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:

```
cmd: <Command> [<Port>] [ack] [<Comment>]
```


The following commands are supported:

Commands	Option	Description
<Command>	get statuspage	sends the status page of the print server
	get servicepage	sends the service page of the print server
	get parameters	sends the parameter list of the print server
	get jobhistory	sends the job history
	get pagecounter	sends the number of printed pages
	set parameters	sends parameters to the print server The syntax and values can be obtained from the parameter list, see: ⇒ 162. Parameter and value must be entered into the email body; see: ⇒ 27.
	print printa print attachment	Prints the email (text only). Prints the first attachment of an email. See: 'printa'
	update ps	Carries out an automatic update using the software that is attached to the email.
	clean mailqueue	Empties the email printer queue and deletes all entries from the mailbox.
[<Port>] (optional) Default: LP1	LP1 LP2 LP3 LP4 LP5	Defines the port used by print server models with several physical ports for sending data. If no port was defined, the default value 'LP1' will be used. - LPT1 or USB1 - LPT2 or USB2 - LPT3 or USB3 (connected via USB hub) - COM1 or USB4 (connected via USB hub) - USB5 (connected via USB hub)
[ack] (optional)	-	sends an acknowledgment back to the sender
[<Comment>] (optional)	-	Freely definable text for descriptions.

The following applies for the instructions:

- not case-sensitive
- one or more space characters are allowed
- max. length is 128 byte
- only the ASCII format can be read.



For a perfect text output of your emails and attachments, make sure that the text encoding of the printer corresponds to that of the email client.

Security

If you want to change parameters or do an update for print servers that have a write protection (see: ⇨ 84), you also need a password. Enter the password into the first line of the email body. Note the following syntax:

```
password: <password>
```

Parameter Changes

Parameter changes are integrated into the email body with the following syntax:

```
<parameter> = <value>
```

The syntax and values can be obtained from the parameter list, see: ⇨ 162.

Example 1

This email causes the print server to send the parameter list to the sender of the email.

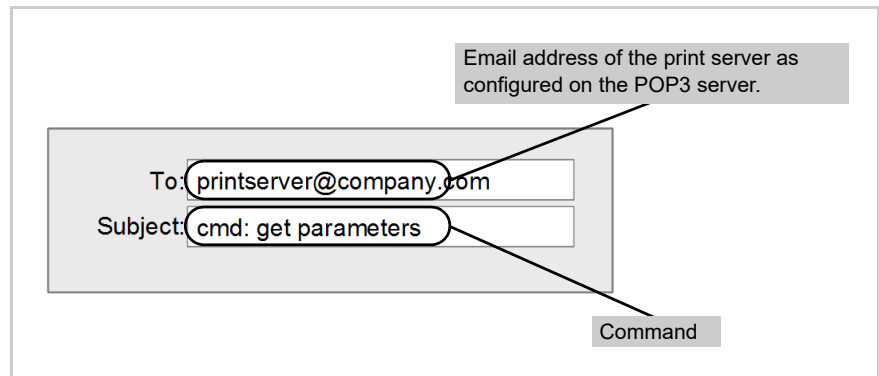


Fig. 3: Administration via Email - Example 1

Example 2

This email causes the printer that is connected to the port 'LPT2' or 'USB2' of the print server to print the attachment of the email. The

sender also receives an acknowledgment of receipt by the print server.

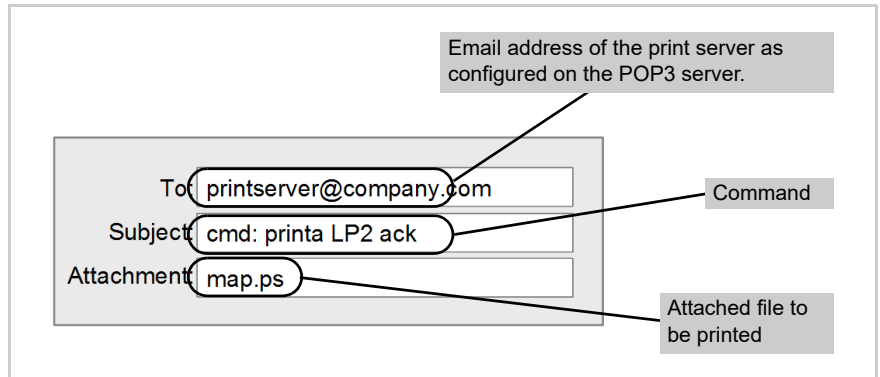


Fig. 4: Administration via Email - Example 2

4 Network Settings



You can define various settings for an ideal integration of the print server into a network. This chapter explains which network protocols and settings are supported by the print server.

What Information Do You Need?

- 'How to Configure IPv4 Parameters' ⇨ 31
- 'How to Configure IPv6 Parameters' ⇨ 34
- 'How to Adapt the Network Speed' ⇨ 37
- 'How to Configure NetBIOS/WINS' ⇨ 38
- 'How to Configure the DNS' ⇨ 40
- 'How to Configure Bonjour' ⇨ 41
- 'How to Use SNMP' ⇨ 43
- 'How to Configure POP3 and SMTP' ⇨ 43
- 'How to Configure WLAN' ⇨ 47

4.1 How to Configure IPv4 Parameters


TCP/IP (Transmission Control Protocol over Internet Protocol) forwards data packets across several connections and establishes a connection between the network participants.


The boot protocols DHCP and BOOTP belong to the TCP/IP protocol family. You can define various IPv4 parameters for an ideal integration of your print server into a TCP/IP network. For further information about the IP configuration, see: ⇨ 7.

What do you want to do?

- 'Configuring IPv4 Parameters via the Print Server Homepage' ⇨ 32
- 'Configuring IPv4 Parameters via the InterCon-NetTool' ⇨ 33

Configuring IPv4 Parameters via the Print Server Homepage

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – TCP/IP.**
3. *Configure the TCP/IP parameters; see: Table 2* ⇨  **32.**
4. *Click Save to confirm.*


 The settings are saved.

Table 2: TCP/IP Parameters

Parameters	Description
IP address	IP address of the print server
Subnet Mask	Subnet mask of the print server
Gateway	Gateway address of the print server
Multicast router as gateway	If this parameter has been enabled, it will be attempted to automatically enter the address of the found multicast router as gateway address. If disabled, the gateway address has to be entered manually.
Host name	Host Name of the print server
Contact person	Freely definable description
Location	Freely definable description
DHCP BOOTP ZeroConf	Enables/disables the protocols 'DHCP', 'BOOTP', and 'ZeroConf'. <i>Protocols offer various possibilities to save the IP address in the print server.</i> We recommend disabling these options once an IP address has been assigned to the print server.

Requirements

Configuring IPv4 Parameters via the InterCon-NetTool

Wizards facilitate the installation and configuration of print servers via the InterCon-NetTool. You can easily enter the desired IP configuration and save it in the print server using the IP Wizard.

- ☑ The InterCon-NetTool is installed on the client, see: ⇒ 15.
- ☑ The network scan via Multicast has been enabled in the InterCon-NetTool.

📁 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print server in the device list.*
The print server is displayed in the device list under the filter 'ZeroConf' with an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf.
 3. **Select Installation – IP Wizard.**
The IP Wizard is started.
 4. *Follow the instructions of the Wizard.*
- 👉 The settings are saved.

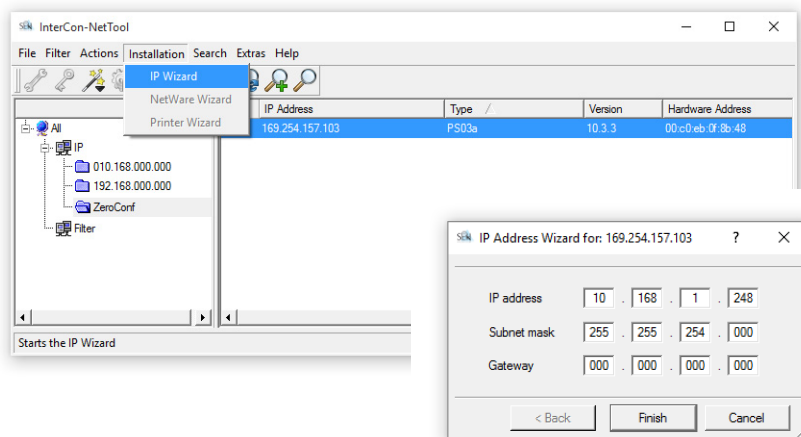


Fig. 5: InterCon-NetTool - IP Wizard

What Are the Advantages of IPv6?

What is the Structure of an IPv6 Address?

4.2 How to Configure IPv6 Parameters

You can integrate the print server into an IPv6 network.

IPv6 (Internet Protocol version 6) is the successor of the more common IPv4. Both protocols are standards for the network layer of the OSI model and regulate the addressing and routing of data packets via a network. The introduction of IPv6 has many benefits:

- IPv6 increases the IP address space from 2^{32} (IPv4) to 2^{128} (IPv6) IP addresses
- Auto Configuration and Renumbering
- Efficiency increase during routing due to reduced header information.
- Integrated services such as IPSec, QoS, Multicast
- Mobile IP

An IPv6 address consists of 128 bits. The normal format of an IPv6 address is eight fields. Each field contains four hexadecimal digits representing 16 bits.

Each field is separated by a colon (:).

Example: fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4

Leading zeros in a field can be omitted.

Example: fe80 : 0 : 0 : 0 : 0 : 10 : 1000 : 1a4

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address.

Example: fe80 : : : : : 10 : 1000 : 1a4

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.

Example: http://[2001:608:af:1::100]:443

Which Types of IPv6 Addresses Are Available?

What do you want to do?



The URL will only be accepted by browsers that support IPv6.

There are different types of IPv6 addresses. The prefixes of the IPv6 addresses provide information about the IPv6 address types.

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many. A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.
- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

- 'Configuring IPv6 Settings via the Print Server Homepage' ⇒ 35
- 'Configuring Logical Printers via the InterCon-NetTool' ⇒ 36
- 'View IPv6 status' ⇒ 55

Configuring IPv6 Settings via the Print Server Homepage

Proceed as follows:

1. Start the Print Server Homepage.
 2. Click **Configuration – IPv6**.
 3. Configure the IPv6 parameters; see: Table 3 ⇒ 36.
 4. Click **Save to confirm**.
- ↪ The settings are saved.


Table 3: IPv6 Parameters


Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the print server.
IPv6 address	Defines a print server IPv6 unicast address assigned manually in the format n:n:n:n:n:n:n:n. Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.
Router	Defines the IPv6 unicast address of the router. The print server sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the print server.

Requirements

Configuring Logical Printers via the InterCon-NetTool

The InterCon-NetTool is installed on the client, see: [⇒ 15](#).

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Settings dialog appears.*
 3. *Click Configuration – IPv6.*
 4. *Configure the IPv6 parameters; see: Table 3 [⇒ 36](#).*
 5. *Click OK to confirm.*
-  The settings are saved.

4.3 How to Adapt the Network Speed

Network communication is done via three direction-oriented transmission methods between two equal data stations. Simplex, half duplex and full duplex.

Duplex Mode

The print server is able to recognize the duplex mode used in the Ethernet and to automatically adjust to it.

The 'Auto' mode is preset. There is also the possibility to manually adjust the setting of the desired duplex mode.





If you set the speed manually, the speed must correspond to the speed of the other network components. It is not possible to operate the print server with full duplex if the hub functions with half duplex, for example.

What do you want to do?

- 'Adapting the Speed via the Print Server Homepage' ⇒ 37
- 'Adapting the Speed via InterCon-NetTool' ⇒ 37

Adapting the Speed via the Print Server Homepage


 Proceed as follows:

1. *Start the Printserver Homepage.*
 2. **Select Configuration – General.**
 3. *Select the desired setting from the Ethernet settings list.*
 4. *Click Save to confirm.*
-  The setting will be saved.

Adapting the Speed via InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list. The Properties dialog appears.*

3. **Select Configuration – General.**
 4. *Select the desired setting from the Ethernet settings list.*
 5. *Click OK to confirm.*
- ↪ The setting will be saved.

4.4 How to Configure NetBIOS/WINS


'NetBIOS' (Network Basic Input Output System) allows you to address a client in Microsoft Windows networks not only via a unique TCP/IP address but also via a unique NetBIOS name.

'WINS' (Windows Internet Naming Service) is a system for the dynamic resolution of NetBIOS names.

- 'Configuring NetBIOS/WINS via the Printserver Homepage' ⇨ 38
- 'Configuring NetBIOS/WINS via InterCon-NetTool' ⇨ 39

Configuring NetBIOS/WINS via the Printserver Homepage

- A WINS server is available in the network.

 Proceed as follows:

1. *Start the Printserver Homepage.*
 2. **Select Configuration – Microsoft Windows.**
 3. *Configure the parameters; see: Table 4 ⇨ 38.*
 4. *Click Save to confirm.*
- ↪ The settings are saved.

Table 4: Microsoft Windows Parameters

Parameters	Description
NetBIOS	Enables/disables peer-to-peer printing.
NetBIOS name	Print Server name Appears in the relevant workgroup or domain.
NetBIOS domain	Name of an existing workgroup or domain.

Benefits and Purpose

What Do You Want to Do?


Requirements


Requirements

Parameters	Description
NetBIOS refresh every	Time interval (in minutes) for updating the NetBIOS parameters.
WINS registration	Enables/disables the WINS services.
WINS via DHCP	Enables/disables the entry of the IP address of a WINS server via DHCP. If the option is disabled, you can enter the IP address of the WINS server manually.
Primary WINS server	IP address of the primary WINS server
Secondary DNS server	IP address of the secondary WINS server

Configuring NetBIOS/WINS via InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- A WINS server is available in the network.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration - Microsoft Windows.**
 4. *Configure the parameters; see: Table 4 ⇒ 38.*
 5. *Click OK to confirm.*
-  The settings are saved.

4.5 How to Configure the DNS

DNS is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa. If a DNS server is available in your network, you can use DNS for your print server.

Benefits and Purpose

If you use a domain name during the configuration process, you must first enable and configure DNS. DNS is used for the configuration of the time server, for example.


What do you want to do?

- 'Configuring DNS via the Print Server Homepage' ⇒ 40
- 'Configuring DNS via the InterCon-NetTool' ⇒ 41

Requirements

Configuring DNS via the Print Server Homepage

- A DNS server is available in the network.

 Proceed as follows:


1. Start the *Printserver Homepage*.
 2. Select **Configuration – DNS**.
 3. Configure the *DNS parameters*; see: *Table 5* ⇒ 40.
 4. Click **Save** to confirm.
-  The settings are saved.


Table 5: DNS parameters


Parameters	Description
DNS	Enables/disables the name resolution via a DNS server.
Domain name	Defines the domain name of an existing DNS server.
Primary DNS server	Defines the IP address of the primary DNS server.
Secondary DNS server	Defines the IP address of the secondary DNS server. The secondary DNS server is used if the first one is not available.

Requirements

Configuring DNS via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ 15.
- A WINS server is available in the network.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration – DNS.**
 4. *Configure the DNS parameters; see: Table 5 ⇨ 40.*
 5. *Click OK to confirm.*
-  The settings are saved.

4.6 How to Configure Bonjour

'Bonjour' allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks.


The print server uses Bonjour to:

- check the IP address assigned via ZeroConf (⇨ 7).
- match host names and IP addresses
- announce its Bonjour services (printing services, Printserver Homepage)

What do you want to do?

- 'Configuring Bonjour via the Print Server Homepage' ⇨ 41
- 'Configuring Bonjour via the InterCon-NetTool' ⇨ 42
- 'View Bonjour status' ⇨ 55

Configuring Bonjour via the Print Server Homepage

 Proceed as follows:

1. *Start the Printserver Homepage.*
2. **Select Configuration – Bonjour.**

Requirements





3. *Configure the Bonjour parameters; see: Table 6* ⇒  42.
 4. *Click Save to confirm.*
- ↩ The settings are saved.

Table 6: Bonjour Parameters

Parameters	Description
Bonjour	Enables/disables Bonjour.
Bonjour name (LPT1,LPT2...) (USB1,USB2...)	Defines the Bonjour name of the print server. The print server uses this name for its Bonjour services. If no Bonjour name is entered, the default name will be used (printer name@ICxxxxxx). You can enter a maximum of 63 characters. The name must not start with an underscore. (As for print servers with several physical printer ports, each port can have a name).

Configuring Bonjour via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒  15.
-  Proceed as follows:
1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. **Select Configuration – Bonjour.**
 4. *Configure the Bonjour parameters; see: Table 6* ⇒  42.
 5. *Click OK to confirm.*
- ↩ The settings are saved.

4.7 How to Use SNMP

SNMP (Simple Network Management Protocol) has become the standard protocol for the administration and monitoring of network elements. The protocol controls communication between the monitored devices and the monitoring station.

SNMP allows you to read and edit management information provided by the network elements. The collection of management information of a device is called MIB.

Private MIB of the Print Server

The print server provides the standard 'MIB-II' and a 'private MIB' (Management Information Base). All print server parameters and status information are saved in the 'private MIB'. The 'private MIB' is saved in the print server on delivery and can be installed immediately.

Benefits and Purpose

The print server parameters can be queried and configured by a management tool by means of the SNMP protocol.

Requirements

- The print server is connected to the network and the printer.
- The print server is known to the network via its IP address, see: ⇒ [7](#).



For more information, read the manual of your SNMP management tool.

4.8 How to Configure POP3 and SMTP

You must configure the protocols POP3 and SMTP on the TPR so that the notification service (⇒ [77](#)) and the administration via email (⇒ [19](#)) will work properly.

POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server. POP3 is used in print servers to administer print servers via email; see: ⇒ [19](#).

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is used in print servers to

What Do You Want to Do?


Requirements

administer print servers via email (see: ⇨ [19](#)) and to send printer information via email (see: ⇨ [77](#)).

- 'Configuring POP3 via the Print Server Homepage' ⇨ [44](#)
- 'Configuring POP3 via the InterCon-NetTool' ⇨ [45](#)
- 'Configuring SMTP via the Printserver Homepage konfigurieren' ⇨ [45](#)
- 'Configuring SMTP via the InterCon-NetTool' ⇨ [47](#)
- 'View POP3/SMTP status' ⇨ [55](#)

Configuring POP3 via the Print Server Homepage

- The print server is set up as user with its own email address on a POP3 server.

 Proceed as follows:

1. *Start the Printserver Homepage.*
2. **Select Configuration – Mail.**
3. *Configure the POP3 parameters; see: Table 7 ⇨ [44](#).*
4. *Click Save to confirm.*


 The settings are saved.


Table 7: POP3 Parameters


Parameters	Description
POP3	Enables/disables the POP3 functionality.
Server name	Defines the POP3 server via the IP address or the host name. The host name can only be used if a DNS server was configured beforehand.
User name	Defines the user name used by the print server to log on to the POP3 server.
Security	Defines the authentication method (APOP/SSL/TLS).
Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.



Requirements

Parameters	Description
Server port	Defines the port used by the print server for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
Password	Defines the password used by the print server to log on to the POP3 server.
Delete read messages	Enables/disables the automatic deletion of read emails.
Ignore mail exceeding	Defines the maximum email size (in KByte) to be accepted by the print server. (0 = unlimited)

Configuring POP3 via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see:  15.
- The print server is set up as user with its own email address on a POP3 server.


 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.
The Properties dialog appears.*
 3. **Select Configuration - Mail - POP3.**
 4. *Configure the POP3 parameters; see: Table 7  44.*
 5. *Click OK to confirm.*
-  The settings are saved.


Requirements

Configuring SMTP via the Printserver Homepage konfigurieren

- The print server is set up as user with its own email address on a POP3 server.

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration - Mail - SMTP.**

3. *Configure the SMTP parameters; see: Table 8* →  **46**.
 4. *Click Save to confirm.*
- 👉 The settings are saved.




The SMTP input mask can also be found under **Configuration – Notification – Email Notification**.


Table 8: SMTP Parameters

Parameters	Description
Server name	Defines the SMTP server via the IP address or the host name. The host name can only be used if a DNS server was configured beforehand.
Server port	Defines the port number used by the print server to send emails to the SMTP server. The port number 25 is preset. When using SSL/TLS, enter 995 as port number.
TLS	Enables/disables TLS. The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.
Sender name	Defines the email address used by the print server to send emails. Note: Very often the name of the sender and the user name are identical.
Signature	Defines the signature to be contained in an email generated by the print server. The print server name, serial number and IP address are used as default values. You can enter a maximum of 128 characters. A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified.
Use POP3 settings	Defines whether the POP3 settings for the authentication shall be used or whether different login data (user name and password) shall be used.
User name	Defines the user name used by the print server to log on to the SMTP server.
Password	Defines the password used by the print server to log on to the SMTP server.

Requirements**Configuring SMTP via the InterCon-NetTool**

- ☑ The InterCon-NetTool is installed on the client, see: ⇨ [15](#).
- ☑ The print server is set up as user with its own email address on a SMTP server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration - Mail - SMTP.**
 4. *Configure the SMTP parameters; see: Table 8 ⇨ [46](#).*
 5. *Click OK to confirm.*
-  The settings are saved.

4.9 How to Configure WLAN

The print server 'PS55' is a WLAN device and is operated wirelessly in the network. During the first setup, the print server is embedded into your WLAN network using WPS (Wi-Fi Protected Setup). Quick Installation Guide.

What is WLAN?

WLAN is a radio technology that allows you to establish wireless connections between network components. The WLAN technology is defined as a standard of the IEEE 802.11 family. The PS55 supports the standards IEEE 802.11b, 802.11g and IEEE 802.11n.

The PS55 has additional WLAN parameters; see: ⇨ [49](#). The current connection status is displayed on the Prints Server Homepage under STATUS – Wireless. For further information on the connection state; see: ⇨ [55](#).

WLAN Security

Make sure that no unauthorized user logs on to the Wireless LAN and that no one has access to the Internet or network resources. Your print server offers several security mechanisms.

Default	Mechanism	
	Encryption	Authentication
WEP	WEP (Open System / Shared Key)	---
WEP+EAP	WEP (Open System)	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)
WPA (Personal Mode)	TKIP/MIC	PSK
WPA2 (Personal Mode)	AES-CCMP	PSK
WPA (Enterprise Mode)	TKIP/MIC	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)
WPA2 (Enterprise Mode)	AES-CCMP	EAP (TLS / MD5 / LEAP / TTLS / PEAP / FAST)

WEP

WEP (Wired Equivalent Privacy) is an encryption method according to IEEE 802.11 on the basis of the RC4 encryption algorithm. WEP offers mechanisms for data encryption and authentication. WEP uses a key to encrypt the entire communication. As for encrypted access points, the same WEP key must be used for the access point and the print server.



Some access points convert WEP keys that are entered as ASCII text into arbitrary hexadecimal values. In this case, the WEP keys for the access point and the print server do not match. It is therefore recommended to use hexadecimal WEP keys.



WEP is outdated and not secure. We recommend to use WPA/WPA2.


WPA/WPA2

In contrast to WEP, WPA (Wi-Fi Protected Access) offers enhanced mechanisms for exchanging keys. The exchange key is only used at the beginning of a session. Afterwards a session key is used. The key


is regenerated periodically. The WPA mechanism requires an authentication at the beginning of a connection.

In the 'Personal Mode' authentication is done via the Pre Shared Key (PSK). The PSK is a password with 8–63 alphanumeric characters. The 'Enterprise Mode' uses the EAP authentication method.

An individual 128 bit key is used for data encryption after the authentication. The encryption methods TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) are available for the encryption of data.

 Proceed as follows:

1. *Start the Printserver Homepage.*
2. *Click **Configuration – Wireless**.*
3. *Configure the WLAN parameters; see: Table 9 ⇨ **49**.*
4. *Click **Save** to confirm.*

 The settings are saved.



If the print server changes the network, it may receive a new IP configuration. In that case, the connection to the Printserver Homepage will be interrupted.

Table 9: WLAN Parameters

Parameters	Description
Mode (Communication mode)	Defines the communication mode. The communication mode defines the network structure in which the print server will be installed. Two modes are available: - In the 'ad-Hoc' mode, the print server communicates directly with another WLAN client (peer-to-peer). The 'infrastructure' mode is suitable for setting up large wireless networks with several devices in different rooms. Communication between the devices is done via an access point which is connected to the network. The access point can be protected by encryption or authentication.

Parameters	Description
Network name (SSID)	Defines the SSID. The ID of a wireless network is referred to as SSID (Service Set Identifier) or network name. Each wireless LAN has a configurable SSID in order to clearly identify the wireless network. The SSID is configured in the access point of a Wireless LAN. Each device (PC, print server, etc.) that is intended to have access to the wireless network must be configured using the same SSID.
Channel Frequency range)	<p>Defines the channel (frequency range) on which the entire data communication will be transmitted. The product uses the 2.4 GHz ISM band. A channel has a bandwidth of 22 MHz. The distance between two neighboring channels is 5 MHz. Channel 3 is preset. The parameter 'Channel' can only be configured in the 'Ad-Hoc' mode.</p> <p>Neighboring channels overlap, which can lead to interferences. If several WLANs are operated in a small radius, a distance of at least five channels should exist between two channels.</p> <p>Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.</p>
Roaming	Enables/disables the use of roaming. Roaming refers to the 'moving' of one radio cell to the next. The print server will use the access point that has the strongest signal. If the print server moves towards the sphere of another access point, the print server switches automatically and without loss of connection to the next radio cell. The parameter 'Roaming' can only be configured in the 'Infrastructure' mode.
-dBm	Defines the roaming threshold in -dbm. If the WLAN signal strength exceeds the threshold, the print server searches for a stronger WLAN signal and may switch into a WLAN with better signal strength. The value 65 - dbm is preset. This parameter can only be configured in the 'Infrastructure' mode.
Encryption method	see: 'WLAN Security' ⇒ 48
Authentication method	see: 'Netzwerkauthentifizierung' ⇒ 104

5 Port Settings



This chapter explains how you can improve the interaction between printer and print server by choosing the right port settings.

What Information Do You Need?

- 'How to Enable PJL' ⇨ 51
- 'How to Enable 1284.4/MLC' ⇨ 52
- 'How to Define the Communication Mode' ⇨ 54
- 'How to Configure COM1 Port Settings' ⇨ 55



In order to determine to which port the print data is to be forwarded in the case of print servers with several physical ports, see: 'Wie verwende ich logische Drucker? (Filterfunktionen)' ⇨ 68.

5.1 How to Enable PJL

With PJL (Print Job Language) commands you can get additional printer information such as detailed status information, printer panel readings or printed pages statistics.

Which information (if any) will be displayed depends on the degree in which the printers can interpret PJL commands. Refer to the manual of your printer for further information.

The print server recognizes if a printer supports PJL and displays this on the Print Server Homepage under **Status – Printer Port** in the **Printer emulation** parameter.





The option '1284.4/MLC' may not be enabled at the same time.

What do you want to do?

- 'Enabling PJL via Print Server Homepage' ⇒ 52
- 'Enabling PJL Via InterCon-NetTool' ⇒ 52

Enabling PJL via Print Server Homepage


 Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Configuration – Printer Port.**
 3. *Tick PJL for the relevant printer port.*
 4. *Click Save to confirm.*
-  The setting will be saved.

Enabling PJL Via InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration – Printer Port.**
 4. *Tick PJL for the relevant printer port.*
 5. *Click OK to confirm.*
-  The setting will be saved.

5.2 How to Enable 1284.4/MLC

IEEE 1284.4 defines a transport protocol for a point-to-point link between a client application and a printer or MFP. One physical link allows you to use several logical channels. These channels allow you to simultaneously and independently exchange different data.

Benefits and Purpose

1284.4/MLC optimizes the bidirectional functionality of external interfaces. Using 1284.4/MLC, you can get more detailed printer status information.




The option 'PJM' may not be enabled at the same time.


What do you want to do?

- 'Enabling 1284.4/MLC via the Print Server Homepage' ⇒ 53
- 'Enabling 1284.4/MLC via InterCon-NetTool' ⇒ 53

Enabling 1284.4/MLC via the Print Server Homepage

 Proceed as follows:


1. *Start the Print Server Homepage.*
2. **Select Configuration – Printer Port.**
3. *Tick 1284.4/MLC.*
4. *Click Save to confirm.*

 The setting will be saved.


Enabling 1284.4/MLC via InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list.*
The Properties dialog appears.
3. **Select Configuration – Printer Port.**
4. *Tick 1284.4/MLC.*
5. *Click OK to confirm.*

 The setting will be saved.

5.3 How to Define the Communication Mode

You can define the communication mode between the print server and the printer via the 'Port Mode'.



The port mode is only available for server models with USB or serial interface.

The following communication modes are available:

- Unidirectional: for unidirectional communication
- Bidirectional: for bidirectional communication with advanced options for acknowledgment and diagnostics.

What do you want to do?

- 'Defining the Communication Mode via the Print Server Homepage' ⇒ 54
- 'Defining a Timeout via the InterCon-NetTool' ⇒ 54

Defining the Communication Mode via the Print Server Homepage

Proceed as follows:

1. *Start the Print Server Homepage.*
2. *Select **Configuration – Printer Port**.*
3. *Select the desired mode from the **Port mode list**.*
4. *Click **Save** to confirm.*

The setting will be saved.

Defining a Timeout via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list. The **Properties dialog** appears.*
3. *Select **Configuration – Printer Port**.*

Requirements

4. *Select the desired mode from the Port mode list.*
 5. *Click OK to confirm.*
- ☞ The setting will be saved.


5.4 How to Configure COM1 Port Settings

In the case of print server models with COM1 port (serial port), you can adapt the COM1 interface to your individual needs.

What do you want to do?

- 'Configuring the COM1 Port via the Print Server Homepage' ⇒ 55
- 'Configuring the COM1 Port via InterCon-NetTool' ⇒ 55


Configuring the COM1 Port via the Print Server Homepage

 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – Printer Port.**
 3. *Select the desired settings from the COM1 list boxes; see: Table 10 ⇒ 56.*
 4. *Click Save to confirm.*
- ☞ The setting will be saved.

Configuring the COM1 Port via InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration – Printer Port.**
 4. *Select the desired settings from the COM1 list boxes; see: Table 10 ⇒ 56.*
 5. *Click OK to confirm.*
- ☞ The setting will be saved.

Requirements

Table 10: COM1 parameters

Parameters	Description
Baud rate	Specifies the baud rate for data transfer.
Parity	Specifies the parity bit for the detection of incorrectly transmitted bit sequences (parity check). The following settings are possible: - none = no parity check - even = even parity check - odd = odd parity check
Data bits	Specifies how many data bits will be transferred in one data packet.
Stop bits	Defines the number of stop bits. Stop bits mark the end of a data transfer unit and allow the recipient of a data transfer to synchronize the data flow.
Flow control	Defines the handshake procedure to control the data flow between print server and printer. The following settings are possible: none = handshake is disabled - xon/xoff = software handshake is enabled - dsr/dtr = hardware handshake is enabled - both = software and hardware handshake are enabled

6 Device Settings



You can configure the device time and the device language for the print server and specify a description. This chapter describes the device settings.

What Information Do You Need?

- 'How to Configure the Language of the Device' ⇨ 57
- 'How to Configure the Device Time' ⇨ 58
- 'How to Determine a Description' ⇨ 60

6.1 How to Configure the Language of the Device

You can set the device language of the print server. The Print Server Homepage and the status information (e.g. the status page) are displayed in the device language. The print server supports the following languages:

- English	- Spanish	- Japanese
- German	- Italian	- Korean
- French	- Portuguese	- Chinese (simplified/traditional)


What do you want to do?

- 'Configuring the Device Language via the Print Server Homepage' ⇨ 57
- 'Configuring Logical Printers via the InterCon-NetTool' ⇨ 58



If you only want to change the language of the Print Server Homepage, you can define the language separately, see: ⇨ 13.

Configuring the Device Language via the Print Server Homepage

 Proceed as follows:

1. Start the Print Server Homepage.
2. Select **Configuration – General**.
3. Select the desired language from the Print server language list.
4. Click **Save** to confirm.

↩ The settings are saved.



Refresh the Print Server Homepage for the new language settings to take effect.

Requirements

The InterCon-NetTool is installed on the client, see: ⇒ 15.



Proceed as follows:

1. Start the *InterCon-NetTool*.
2. Double-click the print server in the device list.
The Properties dialog appears.
3. Select **Configuration – General** from the navigation bar.
4. Select the desired language from the **Print server language list**.
5. Click **OK** to confirm.

↩ The settings are saved.

6.2 How to Configure the Device Time

You can control the device time of the print server via a time server (SNTP server) in the network. A time server synchronizes the time of devices within a network. In the print server, the time server is defined via the IP address or the host name.

Benefits and Purpose

If the time server is activated, all print jobs that are handled by the print server will get a time stamp. Date and time are then displayed under (⇒ 81) 'Job History'.

UTC

The print server uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard.

Time zone

The time received by the time server does not necessarily correspond to your local time zone. Deviations from your location and the resulting time difference (including country-specific particularities such as Daylight Saving Time) can be handled by means of the 'Time zone' parameter.


What do you want to do?


- 'Configuring the Device Time via the Print Server Homepage' ⇒ 59
- 'Configuring Logical Printers via the InterCon-NetTool' ⇒ 59

Requirements

Configuring the Device Time via the Print Server Homepage

- A time server is integrated into the network.


 Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Configuration – Time.**
 3. *Tick SNTP.*
 4. *Into the Time server box, enter the IP address or the host name of the time server*
(The host name can only be used if a DNS server was configured beforehand.)
 5. *Select the code for your local time zone from the Time zone list.*
 6. *Click Save to confirm.*
-  The settings are saved.

Requirements

Configuring Logical Printers via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- A time server is integrated into the network.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. **Select Configuration – Time from the navigation bar.**
 4. *Tick SNTP.*
 5. *Into the Time server box, enter the IP address or the host name of the time server*
(The host name can only be used if a DNS server was configured beforehand.)
 6. *Select the code for your local time zone from the Time zone list.*
 7. *Click OK to confirm.*
-  The settings are saved.


6.3 How to Determine a Description


You can assign freely definable descriptions to the print server or printer. This gives you a better overview of the devices available in the network.

What do you want to do?

- 'Determining Descriptions via the Print Server Homepage' ⇒ 60
- 'Configuring Logical Printers via the InterCon-NetTool' ⇒ 60

Determining Descriptions via the Print Server Homepage


 Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Configuration – General.**
 3. *Enter freely definable names for Description and Dealer.*
 4. *Into the Dealer URL box, enter the website of your print server retailer or seller.*
 5. *Click Save to confirm.*
-  The data is saved.

Configuring Logical Printers via the InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. **Select Configuration – General** from the navigation bar.
 4. *Enter freely definable names for Description and Dealer.*
 5. *Into the Dealer URL box, enter the website of your print server retailer or seller.*
 6. *Click OK to confirm.*
-  The data is saved.

7 Print Server Status Information



The print server can display status information. This chapter describes which status information is available and how to display and read this information.

What Information Do You Need?

- 'How to View Status Information' ⇨ 61
- 'What Status Information is Shown?' ⇨ 62
- 'How to Print a Status or Service Page' ⇨ 64



The LEDs of the print server show its status. Please refer to the 'Quick Installation Guide' for detailed information.

7.1 How to View Status Information

You can view print server status information.

What do you want to do?

- 'Viewing Status Information via the Print Server Homepage' ⇨ 61
- 'Viewing the Status Information via the InterCon-NetTool' ⇨ 62

Viewing Status Information via the Print Server Homepage




Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select the desired menu item from the navigation bar in the Status category.*
- ↪ The status information is shown.

Requirements**Viewing the Status Information via the InterCon-NetTool**

The InterCon-NetTool is installed on the client, see: ⇨ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list. The Properties dialog appears.*
3. *Select the desired menu item from the navigation bar in the Status category.*

⇨ The status information is shown.

7.2 What Status Information is Shown?

This chapter gives an overview of the print server status information. Different status information is available depending on your print server model.

General Status

The **General** page shows status information, such as the name of the print server, the hardware address, and the serial and version numbers, network type etc. The text which you previously entered under 'Configuration - General' will now appear under 'Description.' A description is freely definable and can be used to gain a better overview of the print servers and printers in the system.

WLAN Status

The **WLAN** page contains information about the current WLAN settings.

- 'Connection Status' indicates the status of the network connection.
 - 'Ad hoc': The print server is in ad hoc mode.
 - 'Infrastructure': The print server is in infrastructure mode.
 - 'Out of Range': The print server is logged onto an access point in the infrastructure mode and this access point cannot be reached because it has been turned off, for example.
 - 'Searching': The print server is searching for an access point.
- 'Current network name' indicates the name (SSID - Service Set Identifier) of the WLAN.
- 'Speed' indicates the data transfer rate.
- 'Level' indicates the strength of the signal.

- 'Manufacturer' indicates the manufacturer of the WLAN module.
- 'Wi-Fi Protected Setup (WPS)' shows whether the WPS-Modus is en- or disabled.

Printer Port Status

The **Printer Port** page contains information about the connected printers. The page includes information about the manufacturer, the printer model or the total number of printed pages. The printer operating panel and printer status messages can also be displayed. The information that can be shown depends on the printer and print server model. As for print servers with several physical printer ports, the information is displayed separately for each port.

IPv6 Status

The **IPv6** page shows assigned IPv6 addresses. The print server obtains IPv6 addresses if it is connected to a network that supports IPv6. (Only available on the Print Server Homepage.)

IPsec Status

The **IPsec** page shows the entries of the Internet Protocol Security in the Security Association Database (SAD) and the Security Policy Database (SPD). The 'racoon' logging information is also displayed.

Bonjour Status

The **bonjour** page displays the bonjour name. As for print servers with several physical printer ports, the bonjour name is displayed separately for each port.

Mail Status

The **Mail** page shows the status of the POP3 and SMTP settings.

- 'Mails fetched' shows the number of received emails.
- 'Last POP3 error' shows the last POP3 error.
- 'Next check for mails in' shows the time left till the next mail scan.
- 'Mails sent' shows the number of sent emails.
- 'Last SMTP error' shows the last SMTP error.

Job History

The **Job History** page displays information about the print jobs that have been sent to the print server. A maximum of 64 print jobs are displayed. From the 65th print job onwards the FIFO method (first-in, first-out) is applied. The saved print jobs will be deleted when the print server or printer is turned off or reset. The print jobs will not be deleted when the print server is restarted. The information that is

shown depends on the connected printer model. For a more detailed description, see: see: Table 14 ⇨ 81.

7.3 How to Print a Status or Service Page

You can print status or service pages.

Status Page

A status page contains important, basic print server information such as the print server type, MAC address, etc. Status pages are printed in the print server device language (⇨ 50).

Service page

A service page contains basic print server information as well as a list of the current print server parameter values. Service pages are available in English.

Data format

Before a status or service page can be printed, you need to define the data format of the page. The data formats ASCII, PostScript, DATA-MAX (label printer), and Citizen-Z (label printer) are available. The preset 'Auto' mode automatically uses the appropriate data format.




A status or service page can only be printed if the printer supports one of these data format: ASCII, PostScript, DATAMAX, or Citizen-Z.


What do you want to do?

- 'Defining the Data Format via the Print Server Homepage' ⇨ 65
- 'Defining a Data Format via the InterCon-NetTool' ⇨ 65
- 'Defining a Data Format via the InterCon-NetTool' ⇨ 65
- 'Printing the Status Page via an FTP Connection' ⇨ 66
- 'Printing the Status Page via the Button' ⇨ 66
- 'Printing the Service Page via the Button' ⇨ 66
- 'Printing the Service Page via an FTP Connection' ⇨ 67

Requirements


Defining the Data Format via the Print Server Homepage


 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – General.**
 3. *Select the desired data format from the Status page mode list.*
 4. *Click Save to confirm.*
-  The setting will be saved.

Defining a Data Format via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see:  15.


 Proceed as follows:


1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. **Select Configuration – General.**
 4. *Select the desired data format from the Status page mode list.*
 5. *Click OK to confirm.*
-  The setting will be saved.

Requirements

Defining a Data Format via the InterCon-NetTool


- The InterCon-NetTool is installed on the client, see:  15.


 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print server from the device list.*
 3. **Select Actions – Print Status Page** from the menu bar.
 4. *(Depending on the print server model, you may be asked to specify the printer port. Select the printer port and confirm by clicking Next.)*
 5. **Click Finish.**
-  The status page is printed.

Printing the Status Page via an FTP Connection


Using an FTP connection, you can download a status page to your local computer and print it.


 Proceed as follows:

1. *Change to the directory in which you wish to save the file.*
 2. *Open an FTP connection to the print server:*
Syntax: ftp <IP address>
Example: ftp 192.168.0.123
 3. *Enter an arbitrary user name.*
 4. *Enter the print server password or press the enter key if no password has been assigned.*
 5. *Transfer the status page from the print server to your local computer:*
`get statuspage`
 6. *Close the FTP connection:*
`quit`
 7. *Open and print the file using any text editor.*
-  The status page will be printed.

Printing the Status Page via the Button


Using the button of the print server operating panel, you can print a status page.


 Proceed as follows:

1. *Press the button for a short time.*
-  The status page is printed.

Printing the Service Page via the Button


Using the button of the print server operating panel, you can print a service page.


 Proceed as follows:

1. *Press the button for five seconds.*
-  The service page is printed.

Printing the Service Page via an FTP Connection

Using an FTP connection, you can download a service page to your local computer and print it.

 Proceed as follows:

1. *Change to the directory in which you wish to save the file.*
 2. *Open an FTP connection to the print server:*
Syntax: ftp <IP address>
Example: ftp 192.168.0.123
 3. *Enter an arbitrary user name.*
 4. *Enter the print server password or press the enter key if no password has been assigned.*
 5. *Transfer the service page from the print server to your local computer:*
get servicepage
 6. *Close the FTP connection:*
quit
 7. *Open and print the file using a text editor.*
-  The service page is printed.

8 Print Jobs and Print Data



This chapter contains information concerning the administration of print jobs and print data. You will learn how to load and assign print jobs directly to the print server, how to time print jobs, and how to modify and convert print data.

What Information Do You Need?

- 'How to Define a Timeout for Taking on Print Jobs' ⇨ 68
- 'How to Assign Print Jobs Directly' ⇨ 69
- 'How to Modify Print Data' ⇨ 71
- 'How to Convert Print Data' ⇨ 72
- 'How to Use Logical Printers (Filter Functions)' ⇨ 73

Benefits and Purpose

8.1 How to Define a Timeout for Taking on Print Jobs

You can restrict the acceptance of print jobs to a certain period of time (timeout). If the print server does not receive any print job within the specified time frame, the connection between will be interrupted.

A timeout limits the duration of a connection and thus allows other connections to establish.

What Do You Want to Do?

- 'Defining a Timeout via the Printserver Homepage' ⇨ 68
- 'Defining a Timeout via the InterCon-NetTool' ⇨ 69

Defining a Timeout via the Printserver Homepage

Proceed as follows:


1. *Start the Print Server Homepage.*
2. **Select Configuration – General.**
3. *Enter the time frame in seconds after which the connection will be aborted into the Job receive timeout box.
We recommend to set the value to '120'. (0 s = off)*

Requirements

4. *Click Save to confirm.*
- ↳ The setting will be saved.

Defining a Timeout via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. **Select Configuration – General.**
 4. *Enter the time frame in seconds after which the connection will be aborted into the Job receive timeout box.*
We recommend to set the value to '120'. (0 s = off)
 5. *Click OK to confirm.*
- ↳ The setting will be saved.

8.2 How to Assign Print Jobs Directly

You can assign print jobs directly to the printers via the print server without having to open the file-specific application software.

The print file can be assigned via the Printserver Homepage or the InterCon-NetTool.

The print file must be in a format that suits the printer. When a print file is downloaded to the print server, the file is automatically recognized as print file and printed.




Make sure that the logical printer does not convert data (e.g. ASCII to PostScript), see: ⇒ 73.


What do you want to do?

- 'Assigning the Print File via the Print Server Homepage' ⇒ 70
- 'Assigning the Print File via the InterCon-NetTool' ⇒ 70

Requirements


Assigning the Print File via the Print Server Homepage


 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Actions – Download Area.**
 3. **Select File Printing.**
 4. *Select a logical printer from the list.*
 5. **Click Browse.**
 6. *Select the print file.*
 7. **Click Print.**
 8. *(Enter the print server password, if necessary.)*
-  The print file is printed.

Assigning the Print File via the InterCon-NetTool

The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print servers in the device list to which you want to download a print file.*
 3. **Select Actions – Download – Print File from the menu bar.**
The File Download dialog appears.
 4. **Click Choose.**
 5. *Select the print file.*
 6. *Define how to continue with the passwords:*
 - *If the print servers displayed in the list are not password-protected, activate 'Ask for each password'.*
 - *If the print servers displayed in the list are protected by different passwords, activate 'Ask for each password'.*
 - *If the print servers displayed in the list are protected by the same password, activate 'Use this password' and enter the password.*
 7. **Click Start download.**
 8. *Confirm the security query.*
 9. *(Enter the print server password, if necessary.)*
-  The print file is printed.

8.3 How to Modify Print Data

The print server offers several filter functions for the subsequent editing of print data.

Filter Function 'Find and Replace'

You can use the filter function 'Find and Replace' to edit print data subsequently. For this purpose the print server scans incoming print data streams for specific patterns. As soon as such a pattern is found it will be automatically deleted or replaced by another previously defined pattern.

Benefits and Purpose

It may be useful to edit print data if there is no access to the original documents or if changes to the original files would be too laborious.

You can edit print data using the filter 'Find and Replace'. The filter functions can be configured by means of logical printers, see: ⇒ 73.

Syntax

You can enter various patterns into the boxes 'Find' and 'Replace'. Please pay attention to the following syntax:

- 256 characters can be used.
- You can define various patterns. Use the double semicolon '::' as separator. The first pattern that is defined by separators in the 'Find' string will be replaced by the first pattern that is defined by separators in the 'Replace' string.
- In the case of patterns with ASCII text, you can use clear text (depending on the printer driver, etc.).
- Patterns including escape sequences and control characters (e.g. Postscript or PCL) require special representation. Patterns for hexadecimal code (or other) must be entered as decimal code. In decimal code, each character is represented as three digits (triplets). Each triplet is preceded by a backslash '\'.

Example

The string 'white' is to be replaced by the string 'black' and the string 'cat' is to be replaced by 'dog' in the print data.

	ASCII	Decimal	Hexadecimal
Search	white;;cat	\119\104\105\116\101;;\099\097\116	77 68 69 74 65 63 61 74
Replace	black;;dog	\098\108\097\099\107;;\100\111\103	62 6C 61 63 6B 64 6F 67

Filter Function 'Job Start and Job End'

The print server allows the sending of start and end sequences before/after a print job. These sequences may consist of PRESCRIBE or ESC commands that trigger a form feed after the print job.

ESC commands consist of job start sequence '\027' followed by the actual control characters preceded by a backslash and written as a decimal. Job end sequence '\027 \012', for example, triggers a form feed after the print job. For more information, please look up the available ESC commands in your printer manual.

Configuration is done via logical printers, see: ⇒ [73](#).

8.4 How to Convert Print Data

The print server offers many filters in order to convert print data.

Filter Function 'ASCII / PostScript'

The print server supports the conversion of print data from ASCII to PostScript format. Configuration is done via logical printers, see: ⇒ [73](#).

Filter Function 'HEX Dump Mode' (Hexadecimal + ASCII)

The print server supports the hex dump mode. The hex dump mode is used to search for errors in print data in order to detect communication problems between the computer and the printer.

The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way. Configuration is done via logical printers, see: ⇒ [73](#).

What Are Logical Printers?

Functions of Logical Printers

Filter Function 'LF / CR+LF'

Depending on the system, line breaks are coded differently. In order to get the desired result, the print server supports the conversion of print data from LF (Line Feed) to CR+LF (Carriage Return with Line Feed). Configuration is done via logical printers, see: ⇒ 73.

8.5 How to Use Logical Printers (Filter Functions)

Logical printers are pre-installed filters that are assigned to a print object. The filter contains information about the use of print data.

The print data that is received by the print server will be interpreted and processed depending on the filter settings. This way, print data flows can be manipulated, converted, and sent via defined TCP/IP ports and printer ports.

Logical printers can be used to adapt the print server to various printing needs and networks. All print server models have eight logical printers.

The following functions can be used via logical printers:

- The **printer port** of print server models with several physical printer ports (COM1, USB1, etc.) is defined via the logical printer.
- The logical printer defines which **TCP/IP port** is used to send the print data.
- Depending on the system, line breaks are coded differently. In order to get the desired result, the print server supports the conversion of print data from LF (Line Feed) to **CR+LF** (Carriage Return with Line Feed).
- The print server supports the **hex dump mode**. The hex dump mode is used to search for errors in print data in order to detect communication problems between the computer and the printer. The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way.

Preset Functions of Print Servers with One Port


- The print server allows the printing of a **banner page** if the LPD protocol is used. ASCII or PostScript can be used to display the banner page.
- The print server supports the conversion of print data from **ASCII** to **PostScript** format.
- The print server supports the printing of **binary PostScript** files.
- The print server allows the sending of **start and end sequences** before/after a print job. These sequences may e.g. consist of PRESCRIBE or ESC commands that trigger a form feed after the print job, see: 'How to Modify Print Data' ⇒ 71.
- The print server supports a **Search and Replace** function. This allows you to search for strings within the print data sent to the print server and to replace the strings, if necessary; see: 'How to Modify Print Data' ⇒ 71.

The following functions of logical printers (no. 1–8) are preset for print servers that have a physical printer port.


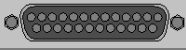
Logical Printer	Preset Function	Preset TCP/IP Port
1	Default settings	9100
2	Conversion of Line Feed (LF) to Carriage Return with Line Feed (CR+LF)	9101
3	Conversion of ASCII into PostScript data	9102
4	Printing a banner page in Novell networks or if the LPD protocol is used	9103
5	Enables the hex dump mode	9104
6	Not assigned	9105
7	Not assigned	9106
8	Not assigned	9107

Preset Printer Ports of Print Servers with Several Printer Ports

The following printer ports of the logical printers (no. 1-8) are preset for print servers that have several physical printer ports.

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
2 X 	1	9100	USB1
	2	9101	USB2
	3	9102	USB3
	4	9103	USB4
	5	9104	USB5
	6	9105	USB1
	7	9106	USB1
	8	9107	USB1

Note:
To some print server models you can connect a hub to USB port 2. In this case, five printers can be administered via USB 1 through 5 by means of the TCP/IP ports.

Physical Printer Ports	Logical Printer	TCP/IP Port	Preset Printer Port
1 X  3 X 	1	9100	LPT1
	2	9101	LPT2
	3	9102	LPT3
	4	9103	COM1
	5	9104	LPT1
	6	9105	LPT1
	7	9106	LPT1
	8	9107	LPT1

How to Use Logical Printers

In order to use the logical printers in an ideal way, you must configure the logical printer with the desired function. Then you must assign the logical printer to a print object. (This procedure can also take place in reversed order.)

What do you want to do?

- 'Configuring Logical Printers via the Print Server Homepage' ⇒ 76
- 'Configuring Logical Printers via the InterCon-NetTool' ⇒ 77
- 'Assigning Logical Printers' ⇒ 77

Configuring Logical Printers via the Print Server Homepage

You can adapt the assigned functions and printer ports to your needs.

Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – Logical Printer.**
 3. *Change the desired parameters, see: Table 11 ⇒ 76.*
 4. **Click Save to confirm.**
- The setting will be saved.

Table 11: Settings of the Logical Printers

Parameters	Description
Start Sequences / End Sequences	Depending on the application, you might have to configure the logical printer.
Search/ Replace	Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings. <i>Wildcards and truncations cannot be used. The string can consist of max. 256 characters.</i>
Hex dump mode	Enables/disables the hex dump mode. The hex dump mode is mainly used to search for errors in print data or lost print data. The hex dump mode displays each character both as hexadecimal code and ASCII character code. Printer control commands are printed as hexadecimal values and do not influence the printout in any way.
CR + LF	Enables/disables the conversion from line feed (LF) to carriage return with line feed (LF+CR).
Banner page	Enables/disables the printing of a banner page if the LPD protocol is used.
ASCII/PostScript	Enables/disables the conversion of ASCII into PostScript data.
Banner page mode	Defines the format (ASCII or PostScript) in which the banner page will be printed.


Requirements

Parameters	Description
TCP/IP Port	TCP/IP port in accordance with the logical printer. The following default values apply: No. 1 = 9100 No. 5 = 9104 No. 2 = 9101 No. 6 = 9105 No. 3 = 9102 No. 7 = 9106 No. 4 = 9103 No. 8 = 9107
Printer Port	Defines the port used by the logical printer for printing. <i>This parameter is only available for print server models with several physical printer ports.</i>
Binary PostScript	Enables/disables the printing of binary PostScript files. 'Binary PostScript' should be enabled if binary PostScript files are to be printed in heterogeneous networks.


Configuring Logical Printers via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ [15](#).

You can adapt the assigned functions and printer ports to your needs.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list.
The Properties dialog appears.*
3. **Select Configuration – Logical Printer.**
4. *Change the desired parameters, see: Table 11 ⇨ [76](#).*
5. *Click OK to confirm.*

 The setting will be saved.

Assigning Logical Printers

Depending on your system, logical printers may be addressed in various ways. The assignment is done when you create printers on the client for the printers connected to the print server (⇨ [9](#)). In Windows, the respective TCP/IP ports are used instead of the logical printers; see: 'TCP/IP-Port' ⇨ [161](#)

9 Printer Status and Printer Messages



The print server can receive information and messages from connected printers and provide these messages/information in various forms. This chapter describes how to display and receive information.

What Information Do You Need?

- 'How to View the Printer Status' ⇨ 78
- 'How to Get Additional Printer Information' ⇨ 80
- 'How to Get Printer Messages via Email' ⇨ 81
- 'How to Get Printer Messages via SNMP Trap' ⇨ 83
- 'How to View the Job History' ⇨ 85

9.1 How to View the Printer Status

There are many ways to keep yourself informed about the status of the printers which are administered via the print server.




The information that can be shown depends on the printer and print server models. As for print servers with several physical printer ports, the information is displayed separately for each port.


What do you want to do?

- 'Displaying the Printer Status and the Printer Display via the Print Server Homepage' ⇨ 79
- 'Configuring Logical Printers via the InterCon-NetTool' ⇨ 79
- 'View the Printer Status via the InterCon-NetTool' ⇨ 80
- 'View printer Status via FTP' ⇨ 80

Requirements**Displaying the Printer Status and the Printer Display via the Print Server Homepage**


 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Status – Printer Port.**

 The printer status and the printer display are displayed.

Configuring Logical Printers via the InterCon-NetTool

The InterCon-NetTool is installed on the client, see:  15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the printer/print server from the device list.*
3. **Select Actions – Printer Panel** from the menu bar.

 The printer panel will be displayed.

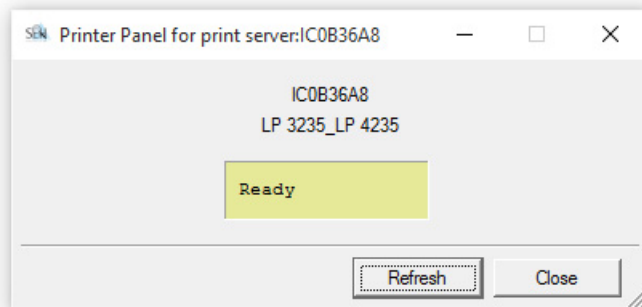



Fig. 6: InterCon-NetTool – Printer Operating Panel

Requirements

View the Printer Status via the InterCon-NetTool

- ☑ The InterCon-NetTool is installed on the client, see: ⇨ 15.


The printer status can be viewed in the 'Port Status' column of the device list. Follow these steps in order to get additional information about the printer status:

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.
The Properties dialog appears.*
 3. *Select Status – Printer Port from the navigation bar.*
- ⇨ The printer status will appear on the screen.

View printer Status via FTP

The printer status is stored in the 'printerport' file of the print server. You can view the contents of the file on the screen via FTP.

 Proceed as follows:

1. *Open an FTP connection to the print server:*
Syntax: ftp <IP address>
Example: ftp 192.168.0.123
2. *Enter either the print server password or press the enter key if no password has been assigned.*
3. *Get the printer status from the print server:*
get printerport
4. *Close the FTP connection:*
quit

9.2 How to Get Additional Printer Information

With PJI (Print Job Language) commands you can get additional printer information via the print server, such as detailed status information, printer panel readings or printed pages statistics. To use PJI, see: ⇨ 44.

9.3 How to Get Printer Messages via Email

You can get email notifications from the printers connected to the print server. You can define under which circumstances the printer will prompt a notification.

This allows up to two recipients to get information about the printer status, printer errors (such as Paper empty), the number of pages printed, or print jobs.



The information that can be sent depends on the connected printer model.

What do you want to do?

- 'Configuring Email Notifications via the Print Server Homepage' ⇒ 81
- 'Configuring Email Notifications via the InterCon-NetTool' ⇒ 82

Requirements

Configuring Email Notifications via the Print Server Homepage

- A DNS server has been configured on the print server, see: ⇒ 32.
- SMTP parameters are configured on the print server; see: ⇒ 36.



Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – Notification.**
 3. **Select Email Notification.**
 4. *Configure the notification parameters; see: Table 12 ⇒ 82.*
 5. *Click Save to confirm.*
- ☞ The settings are saved.

Table 12: Parameters for Email Notification


Parameters	Description
Email active	Enables/disables the email notification for recipient 1 or 2.
Email recipient	Defines the email address of the recipient.
Accounting - Job history, time interval (h), jobs	Enables/disables the sending of a notification containing information about the number of print jobs processed by the print server. <i>Notifications can be sent after a defined interval or after a defined number of print jobs. Valid numbers are 1 to 60 print jobs.</i>
Accounting* - (Page Counter, time interval (h), page interval)	Enables/disables the sending of a notification containing information about the number of pages printed by the printer. <i>Notifications can be sent after a defined interval or after a defined number of pages printed.</i>
Printer error* - Paper empty, Paper jam, etc.	Define the type of printer error that will cause a notification.


* In the case of print servers with several physical printer ports, you must select the relevant port.

Requirements

Configuring Email Notifications via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ [15](#).
- A DNS server has been configured on the print server, see: ⇨ [32](#).
- SMTP parameters are configured on the print server; see: ⇨ [36](#).

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server or printer in the device list. The Properties dialog appears.*
 3. **Select Configuration – Notification from the menu bar.**
 4. **Select Email Notification.**
 5. *Select the tab of the relevant recipient.*
 6. *Configure the notification parameters; see: Table 12 ⇨ [82](#).*
 7. **Click OK to confirm.**
-  The settings are saved.

9.4 How to Get Printer Messages via SNMP Trap

You can get SNMP trap notifications from the connected printers. You can define under which circumstances the printer will prompt a notification.

This allows two recipients to get information about the printer status, printer errors (such as Paper empty), the number of pages printed, or print jobs.



The information that can be shown depends on the connected printer model.

What do you want to do?

- 'Enabling SNMP Trap Notifications via the Print Server Homepage' ⇒ 83
- 'Configuring SMTP Notifications via the InterCon-NetTool' ⇒ 84

Enabling SNMP Trap Notifications via the Print Server Homepage

Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select **Configuration – Notification**.*
 3. *Select **SNMP Trap Notification**.*
 4. *Configure the notification parameters; see: Table 13 ⇒ 84.*
 5. *Click **Save** to confirm.*
- The settings are saved.

Table 13: Parameters for SNMP Trap Notification


Parameters	Description
IP address	Defines the IP address of the recipient.
Trap community	Defines the trap community of the recipient.
Authentication traps	Enables/disables the sending of authentication traps.
Printer traps	Enables/disables the sending of traps in case of an error.
Printer error* - Paper empty, Paper jam, etc.	Defines the printer errors that will cause a notification.


* In the case of print servers with several physical printer ports, you must select the relevant port.

Requirements

Configuring SMTP Notifications via the InterCon-NetTool

The InterCon-NetTool is installed on the client, see: ⇨ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server or printer in the device list. The Properties dialog appears.*
 3. **Select Configuration – Notification.**
 4. **Select SNMP Trap Notification.**
 5. *Select the tab of the relevant recipient.*
 6. *Configure the notification parameters; see: Table 13 ⇨ 84.*
 7. *Click OK to confirm.*
-  The settings are saved.

9.5 How to View the Job History

Information on the print jobs handled by the print server are registered and shown in the job history.

A maximum of 64 print jobs are displayed. From the 65th print job onwards the FIFO method (first-in, first-out) is applied. The saved print jobs will be deleted when the print server or printer is turned off or reset. The print jobs will not be deleted when the print server is restarted.

Depending on the connected printer model, the following information is shown in the job history:

Table 14: Job History - Status Information

Parameters	Description
No.	Number of the print job.
Status	<p>Status of the print connection. The following statuses are possible:</p> <ul style="list-style-type: none"> • 'Pending' means that the print job has been accepted by the print server but that the data transfer has not yet started. • 'Processing' means that the print job has been transferred from the print server to the printer. • 'Processing stopped' means that the data transfer to the printer was interrupted. This can occur if, for example, the printer ran out of paper. If the printer error is fixed, data transfer will be resumed. • 'Completed' means that the print server has completely forwarded the print job to the printer. • 'Aborted' means that the print job has been aborted. This can occur if, for example, the print server has been restarted while the print job was processed.
Printer port	<p>Port that is used for printing.</p> <p><i>This parameter is only available for print server models with several physical printer ports.</i></p>
Protocol	Protocol used to transfer the print data.
Name	Job names of print jobs using the protocols HTTP, IPP, LPR and LPD. The string starts with the identification number of the print job, followed by the host name of the device from which the print job has been spooled.
Sender	Sender of the print job (in TCP/IP networks).
Size	Size (in kB) of the print job.
Pages	Number of pages of the print job.

Parameters	Description
Creation time	Time at which the print job has been sent to the print server.
Duration	The time (in seconds) needed by the print server for processing the print job.



A time server (⇒ 51) must be configured on the print server so that the date and time can be displayed correctly. If no time server is configured, the time stamp corresponds to the default time.

What do you want to do?

- 'Displaying the Job History via the Print Server Homepage' ⇒ 86
- 'Displaying the Job History via the InterCon-NetTool' ⇒ 86

Displaying the Job History via the Print Server Homepage

Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select Status – Job History.*
- ↳ The job history is displayed.

Displaying the Job History via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. *Select Status – Job History from the navigation bar.*
- ↳ The job history is displayed.

Requirements

10 Security



A number of security mechanisms are available to ensure optimum security for the print server. This chapter describes how to make use of these security mechanisms.

What Information Do You Need?

- 'How to Define a Password for the Print Server (Read/Write Protection)' ⇒ [1088](#)
- 'How to Disable the HTTP Access (Protection against Viruses)' ⇒ [1089](#)
- 'How to Protect Printers against Unauthorized Access (IP Sender Control)' ⇒ [1090](#)

More security-related topics from other chapters:

- Encrypted printing ⇒ [1018](#)
- Managing certificates in the print server ⇒ [1093](#)
- Authentication of the print server in the network ⇒ [10107](#)
- Authentication of the print server/client if the administrative access to PrintServer Homepage is protected via SSL/TLS ⇒ [10107](#)
- Administering the print server via FTPS connections ⇒ [10117](#)
- Security mechanisms of WLAN print servers ⇒ [1040](#)
- Protecting the print server via Internet Protocol Security (IPsec) ⇒ [10117](#)
- Receiving encrypted ThinPrint® data ⇒ [10139](#)

10.1 How to Define a Password for the Print Server (Read/Write Protection)

Write Protection

A password can protect the print server against unauthorized parameter modifications. If a password was set, you must enter the password before you can save the changes to the parameters. This means that changes to the parameters can only be made using a valid password.


Read protection


In addition, you can protect the display of parameters with a password too. For this purpose, the parameter **Access control** must be enabled. If this parameter is enabled, a password must be entered when opening the Print Server Homepage or the **Properties** dialog via the InterCon-NetTool.

What do you want to do?

- 'Defining the Password via the Print Server Homepage' ⇒ 88
- 'Defining a Timeout via the InterCon-NetTool' ⇒ 88

Defining the Password via the Print Server Homepage


 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select **Configuration - Protection**.*
 3. *Enter a password into the **Password** box in order to enable the write protection.*
 4. *Tick **Access control** in order to define the read protection, if required.*
 5. *Click **Save** to confirm.*
-  The settings are saved.

Defining a Timeout via the InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*

2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. **Select Configuration – Protection.**
 4. *Enter a password into the Password box in order to enable the write protection.*
 5. *Tick Access control in order to define the read protection, if required.*
 6. *Click OK to confirm.*
- ⇒ The settings are saved.



You can also define the password using the menu bar of the InterCon-NetTool. Select **Actions – Change password** from the menu bar.

10.2 How to Disable the HTTP Access (Protection against Viruses)

HTTP (Hypertext Transfer Protocol) is a protocol for the transfer of data. The print server needs HTTP for the data transfer of the Print Server Homepage.

The print server cannot be attacked directly by viruses. Attacks to open ports (e.g. port 80 / HTTP) can have a certain influence on the print server and affect its functions.

To prevent attacks to open ports, you can disable the HTTP protocol on the print server.



The Printserver Homepage is no longer available if HTTP is disabled. In that case, the print server can only be configured via the alternative administration methods; see 'Administrationsmethoden' ⇒ 13.


- 'Disabling HTTP via the Print Server Homepage' ⇒ 90
- 'Enabling or Disabling HTTP via the InterCon-NetTool' ⇒ 90

Benefits and Purpose


What do you want to do?

Requirements

Disabling HTTP via the Print Server Homepage

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration - Protection.**
3. *Clear HTTP.*
4. *Click Save to confirm.*


 The setting will be saved.

Enabling or Disabling HTTP via the InterCon-NetTool


You can disable HTTP via the InterCon-NetTool.

If you disabled HTTP previously, you can enable HTTP via the InterCon-NetTool.

The InterCon-NetTool is installed on the client, see:  15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list.*
The Properties dialog appears.
3. **Select Configuration - Protection.**
4. *Tick/clear HTTP.*
5. *Click OK to confirm.*

 The setting will be saved.

10.3 How to Protect Printers against Unauthorized Access (IP Sender Control)

In TCP/IP networks you can define which IP addresses and thus which workstations are allowed to access a printer and print.

The 'IP Sender Control' allows you to protect printers and sensitive data against unauthorized access and to attribute print costs precisely within the company.

Benefits and Purpose

To enable the 'IP Sender Control', you must enter the IP addresses or host names of the clients into an **IP sender** list. The print server will only accept print jobs from clients specified in the list.

Up to eight IP senders can be specified. The use of wildcards (*) allows you to define subnetworks (e.g. 192.168.122.*) and to authorize these subnetworks for printing.





In order to disable the IP sender control you must enter '*' into the first IP sender box. Once an IP sender has been defined, all undefined clients lose their authorization to print via the print server.

What do you want
to do?

- 'Assigning Authorizations via thePrint Derver Homepage' ⇨ 91
- 'Defining a Timeout via the InterCon-NetTool' ⇨ 91

Assigning Authorizations via thePrint Derver Homepage


 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – Protection.**
 3. *Into the IP sender box, enter the IP addresses or host names of authorized clients.*
(The host name can only be used if a DNS server was configured beforehand.)
 4. *Click Save to confirm.*
-  The settings are saved.

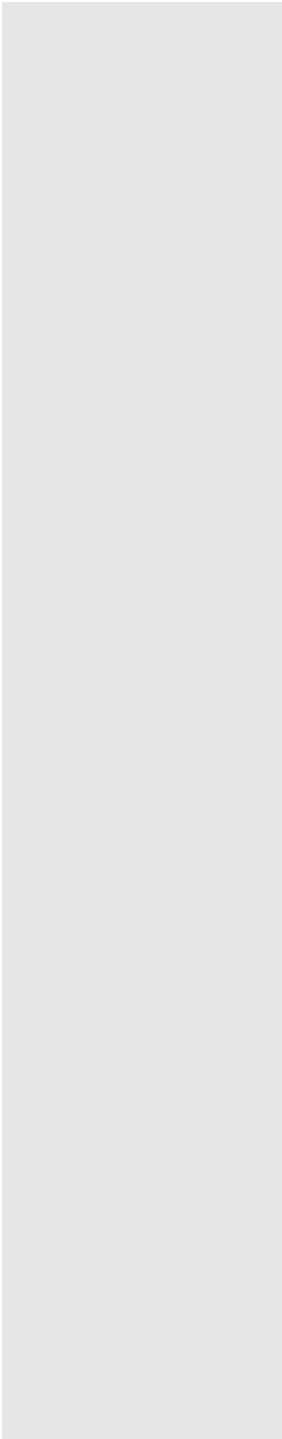
Defining a Timeout via the InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇨ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list.*
The Properties dialog appears.
3. **Select Configuration – Protection from the navigation bar.**

- 
4. *Into the **IP sender** box, enter the IP addresses or host names of authorized clients.*
(The host name can only be used if a DNS server was configured beforehand.)
 5. *Click **OK** to confirm.*
- ↪ The settings are saved.

11 Certificate Management



The print server has its own certificate management. This chapter explains how certificates are used and when the use of certificates is recommended.

What are Certificates?

Certificates can be used in TCP/IP-based networks to encrypt data and to authenticate communication partners. Certificates are electronic messages containing a key (public key) and a signature.

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates in your print server to

- encrypt print data; see: ⇨ [109](#).
- check the identity of the print server in the network; see: ⇨ [1107](#).
- authenticate the print server if the connection to the Printserver Homepage is encrypted via SSL/TLS (HTTPS).
- administer the print server via an FTPS connection; see: ⇨ [117](#).
- allow for a certificate-based authentication of the remote server in the case of IPsec; see: ⇨ [117](#).
- to encrypt ThinPrint data; see: ⇨ [1139](#).



If you want to use certificates, it is advisable to protect the print server by a password so that the certificate cannot be deleted by unauthorized persons, see ⇨ [88](#).

Which Certificates are available?

Both self-signed certificates and CA certificates can be used in the print server. The following certificates can be distinguished:

- Upon delivery, a self-signed certificate (the so-called **default certificate**) is stored in the print server. It is recommended that you replace the default certificate by a self-signed certificate or requested certificate as soon as possible.
- **Self-signed certificates** have a digital signature that has been created by the print server.

What Information Do You Need?

- A **requested certificate** is created by a certification authority (CA) for the print server on the basis of a certificate request.
- **CA certificates** are certificates that have been issued for a certification authority (CA). They are used for verifying certificates that have been issued by the respective certification authority.
- **PKCS#12** certificates are used to save private keys and their respective certificates and to protect them by means of a password.

The following certificates can be installed at the same time in the print server:

- 1 print server certificate, i.e. 1 self-signed certificate or 1 requested certificate or 1 PKCS#12 certificate
- 1–8 CA certificates

- 'How to View Certificates' ⇨ 94
- 'How to Create a Self-Signed Certificate' ⇨ 96
- 'How to Create a Certificate Request for a Requested Certificate' ⇨ 98
- 'How to Save a Requested Certificate in the Print Server' ⇨ 100
- 'How to Save a PKCS12 Certificate in the Print Server' ⇨ 102
- 'How to Save CA Certificates in the Print Server' ⇨ 103
- 'How to Delete Certificates' ⇨ 104
- 'Network Authentication' ⇨ 107

11.1 How to View Certificates

Certificates installed in the print server and certificate requests can be displayed and viewed.

- 'Displaying the Print Server Certificate via the Print Server Homepage' ⇨ 95


What do you want to do?

Requirements


- 'Displaying the Print Server Certificate or Certificate Request via the InterCon-NetTool' ⇨ 95
- 'Displaying the CA certificate via the Print Server Homepage' ⇨ 96
- 'Displaying the CA certificate via the InterCon-NetTool' ⇨ 96

Displaying the Print Server Certificate via the Print Server Homepage

- A certificate request has been created or a client certificate is installed in the print server.

 Proceed as follows:


1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select Print server certificate.**

 The certificate respectively certificate request is displayed.


Displaying the Print Server Certificate or Certificate Request via the InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇨ 15.
- A certificate request has been created or a client certificate is installed in the print server.


 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. **From the Actions menu, select Certificate – Print server certificate.**

 The certificate respectively certificate request is displayed.

Requirements**Displaying the CA certificate via the Print Server Homepage**

- A CA certificate is installed in the print server.

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select CA certificates.**
4. *For the desired certificate select Show.*

↳ The CA certificate is displayed.


Displaying the CA certificate via the InterCon-NetTool

CA certificates can only be displayed via the InterCon-NetTool if 8 CA certificates are installed in the print server. If 7 or less certificates are installed, the dialog for installing a certificate appears (⇒ 103).

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

- 8 CA certificates are installed in the print server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. **From the Actions menu, select Certificate – Root certificate.**

↳ The CA certificate is displayed.


11.2 How to Create a Self-Signed Certificate**What do you want to do?**

- 'Creating Self-Signed Certificates via the Print Server Homepage'
⇒ 97
- 'Creating a Self-Signed Certificate via the InterCon-NetTool'
⇒ 98

Requirements

Creating Self-Signed Certificates via the Print Server Homepage

A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇨ [104](#).

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select Print server certificate.**
4. *Enter the relevant parameters; siehe: Tabelle 15 ⇨ [97](#).*
5. **Click Create self-signed certificate.**


 The certificate will be created and installed.



Tabelle 15: Parameters for the Creation of Certificates


Parameters	Description
Common name	Is used to clearly identify the certificate. It is advisable to use the IP address or the host name of the print server to allow a clear assignment of the certificate to the print server. <i>You can enter a maximum of 64 characters.</i>
Email address	Specifies an email address. <i>You can enter a maximum of 40 characters. (Optional entry)</i>
Organization name	Specifies the company that uses the print server. <i>You can enter a maximum of 64 characters.</i>
Organizational unit	Specifies the department or subsection of a company. <i>You can enter a maximum of 64 characters. (Optional entry)</i>
Location	Specifies the locality where the company is based. <i>You can enter a maximum of 64 characters.</i>
State name	Specifies the state in which the company is based. <i>You can enter a maximum of 64 characters. (Optional entry)</i>
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Specifies the date from which on the certificate is valid.
Expires on	Specifies the date from which on the certificate becomes invalid.



Requirements

Parameters	Description
RSA key length	Defines the length of the RSA key used: <ul style="list-style-type: none"> - 512 bit (fast encryption and decryption) - 768 bit - 1024 bit (standard encryption and decryption) - 2048 bit (slow encryption and decryption)

Creating a Self-Signed Certificate via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ 15.
- A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇨ 104.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print server from the device list.*
 3. *Select Actions – Certificate – Server certificate from the menu bar.*
The Certificate dialog appears.
 4. *Tick Create self-signed certificate.*
 5. *Click Next.*
 6. *Enter the relevant parameters; siehe: Tabelle 15 ⇨ 97.*
 7. *Click Next.*
The parameters are listed.
 8. *Confirm by clicking Next.*
-  The certificate will be created and installed.

11.3 How to Create a Certificate Request for a Requested Certificate

As preparation for using a certificate which is issued by a certification authority for the print server, a certificate request can be created in the print server. The request must be sent to the certification authority which creates an certificate on the basis of this request. The certificate must be in 'base64' format.



After the creation of a certificate request, no print server certificate can be installed until the requested certificate has been saved in the print server.

What do you want to do?

- 'Creating a Certificate Request via the Print Server Homepage' ⇨ [99](#)
- 'Creating a Certificate Request via the InterCon-NetTool' ⇨ [99](#)

Requirements

Creating a Certificate Request via the Print Server Homepage

- A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇨ [104](#).
- A certificate request must not already be created. To delete the certificate request, see: ⇨ [105](#).

Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select Print server certificate.**
4. *Enter the required parameters, siehe: Tabelle 15 ⇨ [97](#).*
5. **Click Create certificate request.**
The creation of the certificate request is in progress.
6. *Save the request as text file.*
7. *Send the text file as certificate request to a certification authority.*


When the requested certificate has been received, it must be saved in the print server; see: ⇨ [100](#).

Requirements

Creating a Certificate Request via the InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ [15](#).
- A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇨ [104](#).

- ☑ A certificate request must not already be created. To delete the certificate request, see: ⇨ 105.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. *Select Actions – Certificate – Server certificate from the menu bar.*
The Certificate dialog appears.
4. *Tick Create certificate request.*
5. *Click Next.*
6. *Enter the relevant parameters; siehe: Tabelle 15 ⇨ 97.*
7. *Click Next.*
The parameters are listed.
8. *Confirm by clicking Next.*
The creation of the certificate request is in progress.
9. *Save the request as text file.*
10. *Send the text file as certificate request to a certification authority.*

When the requested certificate has been received, it must be saved in the print server; see: ⇨ 100.

11.4 How to Save a Requested Certificate in the Print Server

A certificate which is issued by a certification authority for the print server can be used in the print server.

- ☐ 'Saving a Requested Certificate via the Print Server Homepage'
⇨ 101
- ☐ 'Creating a Self-Signed Certificate via the InterCon-NetTool'
⇨ 101


What do you want to do?

Requirements

Saving a Requested Certificate via the Print Server Homepage

A certificate request has been created at an earlier date; see: ⇒ [98](#).

The certificate must be in 'base64' format.

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select Print server certificate.**
4. **Click Durchsuchen.**
5. *Specify the requested certificate.*
6. **Click Load Certificate.**

↳ The requested certificate is saved in the print server.


Creating a Self-Signed Certificate via the InterCon-NetTool

Requirements

The InterCon-NetTool is installed on the client, see: ⇒ [15](#).

A certificate request has been created at an earlier date; see: ⇒ [98](#).

The certificate must be in 'base64' format.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. **Select Actions – Certificate – Server certificate from the menu bar.**
The Certificate dialog appears.
4. **Click '...'**
5. *Specify the requested certificate.*
6. **Click Load.**

↳ The requested certificate is saved in the print server.

What do you want to do?


11.5 How to Save a PKCS12 Certificate in the Print Server

PKCS#12 certificates are used to save private keys and their respective certificates and to protect them by means of a password.

- 'Saving a PKCS#12 certificate via Print Server Homepage' ⇒ 102
- 'Saving a PKCS#12 Certificate via theInterCon-NetTool' ⇒ 102

Saving a PKCS#12 certificate via Print Server Homepage

- A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇒ 104.
- The certificate must be in 'base64' format.


 Proceed as follows:

1. Start the *Print Server Homepage*.
2. Select **Configuration – Certificates**.
3. Select **Print server certificate**.
4. Click **Load certificate (pkcs12 format)**.
5. Click **Durchsuchen**.
6. Enter the certificate.
7. Enter the password.
8. Click **Load PKCS12**.

👉 The PKCS#12 certificate is saved in the print server.

Saving a PKCS#12 Certificate via theInterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- A print server certificate must not be already installed in the print server. To delete a print server certificate, see: ⇒ 104.
- The certificate must be in 'base64' format.

 Proceed as follows:

1. Start the *InterCon-NetTool*.

Requirements

2. *Select the print server from the device list.*
 3. *Select Actions – Certificate – Server certificate from the menu bar.*
The Certificate dialog appears.
 4. *Tick Load certificate (pkcs12 format).*
 5. *Click Next.*
 6. *Enter the certificate.*
 7. *Enter the password.*
 8. *Click Next.*
- ↳ The PKCS#12 certificate is saved in the print server.

11.6 How to Save CA Certificates in the Print Server

In order to check the identity of the network communicating parties of the print server, it is necessary to validate their certificates. For this, the root CA certificates of the certification authorities that have issued the certificates of said communicating parties are installed on the print server.

Up to 8 CA certificates can be saved in the print server. Thus multi-level public key infrastructures (PKIs) are supported.



If you use the authentication method 'EAP-TLS' (⇒ 109), you must install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) in the print server and specify it for the authentication method; see: ⇒ 104.

What do you want
to do?

- 'Saving CA Certificates via the Print Server Homepage' ⇒ 103
- 'Saving a CA Certificate via the InterCon-NetTool' ⇒ 104

Saving CA Certificates via the Print Server Homepage

- The certificate must be in 'base64' format.



Proceed as follows:

1. *Start the Print Server Homepage.*

Requirements

Requirements

2. *Select Configuration – Certificates.*
 3. *Select CA certificates.*
 4. *Click Durchsuchen.*
 5. *Specify the CA certificate.*
 6. *Click Load CA certificate.*
- ☞ The CA certificate is saved in the print server.

Saving a CA Certificate via the InterCon-NetTool



If the maximum of 8 CA certificates is installed in the print server, the dialog for displaying the certificates appears (⇒ 15).

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- The certificate must be in 'base64' format.



Proceed as follows:




1. *Start the InterCon-NetTool.*
 2. *Select the print server from the device list.*
 3. *Select Actions – Certificate – Server certificate from the menu bar.*
The Certificate dialog appears.
 4. *Click '...'*
 5. *Specify the CA certificate.*
 6. *Click Load.*
- ☞ The CA certificate is saved in the print server.

11.7 How to Delete Certificates



Do not delete the certificate (CA/self-signed/PKCS#12) if only HTTPS is defined as the permitted connection type for the web access to the Printserver Homepage. If the certificate is deleted, the Printserver Homepage can no longer be reached via SSL/TLS (HTTPS). In this case, use a non-encrypted connection.

What do you want to do?

- 'Deleting a Print Server certificate or Certificate Request via the Print Server Homepage' ⇒ 105
- 'Deleting a Print Server Certificate or Certificate Request via the InterCon-NetTool' ⇒ 105
- 'Deleting CA Certificates via the Print Server Homepage' ⇒ 106

Deleting a Print Server certificate or Certificate Request via the Print Server Homepage**Requirements**

- A certificate request has been created or a client certificate is installed in the print server.




Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – Certificates.**
3. **Select Print server certificate.**
4. **Click Delete certificate.**

↪ The certificate respectively certificate request is deleted.

Deleting a Print Server Certificate or Certificate Request via the InterCon-NetTool**Requirements**

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- A certificate request has been created or a client certificate is installed in the print server.




Proceed as follows:


1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. **Select Actions – Certificate – Server certificate from the menu bar.**
The Certificate dialog appears.
4. **Click Delete.**

↪ The certificate respectively certificate request is deleted.

Requirements**Deleting CA Certificates via the Print Server Homepage**

A CA certificate is installed on the print server.

 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select **Configuration – Certificates.***
 3. *Select **CA certificates.***
 4. *For the desired certificate select **Show.***
The CA certificate is displayed.
 5. *Click **Delete.***
-  The certificate is deleted.

12 Network Authentication



By means of authentication, a network can be protected against unauthorized access. The print server can participate in various authentication procedures. This chapter describes which procedures are supported and how these procedures are configured on the print server.

What is IEEE 802.1X?

The IEEE 802.1X standard provides a basic structure for various authentication and key management protocols. IEEE 802.1X allows you to control the access to networks. Before users gain access to a network via a network device, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

The standard IEEE 802.1X is based upon the EAP (Extensible Authentication Protocol). EAP is a universal protocol for many authentication procedures. EAP allows for a standardized authentication procedure between the network device and an authentication server (RADIUS). First you must define the authentication procedure (TLS, PEAP, TTLS, etc.) to be used and configure it on all network devices involved.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources.

The print server supports various EAP authentication methods in order to authenticate itself in a protected network.

What Information Do You Need?

- 'How to Configure EAP-MD5' ⇨ 108
- 'How to Configure EAP-TLS' ⇨ 109
- 'How to Configure EAP-TTLS' ⇨ 111
- 'How to Configure PEAP' ⇨ 113
- 'How to Configure EAP-FAST' ⇨ 115

12.1 How to Configure EAP-MD5

Benefits and Purpose

EAP-MD5 validates the identity of devices or users before they gain access to network resources. You can configure the print server for the EAP-MD5 network authentication. This makes sure that the print server gets access to protected networks.

Mode of Operation

EAP-MD5 describes a user-based authentication method via a RADIUS server. The print server must be defined as user (with user name and password) on a RADIUS server. The authentication method EAP-MD5 must then be enabled on the print server and the user name and password need to be entered.

What do you want to do?

- 'Enabling EAP-MD5 via the Print Server Homepage' ⇨ 108
- 'Activating EAP-MD5 via InterCon-NetTool' ⇨ 109



The authentication of print server models with WLAN support is configured via the menu item **Configuration – WLAN**.


Requirements


Enabling EAP-MD5 via the Print Server Homepage

- The print server is defined as user (with user name and password) on a RADIUS server.
- Proceed as follows:
1. *Start the Print Server Homepage.*
 2. **Select Configuration – Protection.**
 3. **Select Authentication.**
 4. **Select EAP-MD5 from the Authentication list.**
 5. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 6. *Click Save to confirm.*
- The settings are saved.

Requirements**Activating EAP-MD5 via InterCon-NetTool**

- ☑ The InterCon-NetTool is installed on the client, see: ⇨ 15.
- ☑ The print server is defined as user (with user name and password) on a RADIUS server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. *Select **Configuration – Protection** from the navigation bar.*
 4. *Select the **Authentication** tab.*
 5. *Select **EAP-MD5** from the Authentication list.*
 6. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 7. *Click **OK** to confirm.*
-  The settings are saved.

Benefits and Purpose**12.2 How to Configure EAP-TLS**

EAP-TLS (Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the print server for the EAP-TLS network authentication. This makes sure that the print server gets access to protected networks.

Mode of Operation

EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between the print server and the RADIUS server. An encrypted TLS connection between the print server and the RADIUS server is established in this process. Both RADIUS server and print server need a valid, digital certificate signed by a CA. The RADIUS server and the print server must validate the certificate. After the mutual authentication was successful, the access to the network will be freed.

Since each device needs a certificate, a PKI (Public Key Infrastructure) must be available. User passwords are not necessary.

Procedure



If you want to use the EAP-TLS authentication, you must observe the following instructions in the indicated order. Otherwise the print server cannot be addressed in the network. In this case you have to reset the print server parameters; see: ⇨ 122.

- Create a certificate request on the print server; see: ⇨ 98.
- Create a certificate using the certificate request and the authentication server (RADIUS).
- Install the requested certificate on the print server; see: ⇨ 100.
- Install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: ⇨ 103.
- Enable the authentication method 'EAP-TLS' on the print server.
 - 'Enabling EAP-TLS via the Print Server Homepage' ⇨ 110
 - 'Activating EAP-TLS via InterCon-NetTool' ⇨ 111



The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Enabling EAP-TLS via the Print Server Homepage



Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration - Protection.**
 3. **Select Authentication.**
 4. **Select EAP-TLS from the Authentication list.**
 5. **Click Save to confirm.**
- ↪ The settings are saved.

Requirements**Activating EAP-TLS via InterCon-NetTool**

☑ The InterCon-NetTool is installed on the client, see: ⇨ 15.

📄 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list. The Properties dialog appears.*
3. *Select **Configuration – Protection** from the navigation bar.*
4. *Select the **Authentication** tab.*
5. *Select **EAP-TLS** from the Authentication list.*
6. *Click **OK** to confirm.*

👉 The settings are saved.

Benefits and Purpose**12.3 How to Configure EAP-TTLS**

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the print server for the EAP-TTLS network authentication. This makes sure that the print server gets access to protected networks.

Mode of Operation

EAP-TTLS consists of two phases:

- In phase 1, a TLS-encrypted channel between the print server and the RADIUS server will be established. Only the RADIUS server authenticates itself using a certificate that was signed by a CA. This process is also referred to as 'outer authentication'.
- In phase 2, an additional authentication method is used for the communication within the TLS channel. EAP-defined methods and older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. Moreover, TTLS supports most authentication protocols.

What do you want to do?

- 'Enabling EAP-TTLS via the Print Server Homepage' ⇨ 112
- 'Activating EAP-TTLS via InterCon-NetTool' ⇨ 112



The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Requirements

Enabling EAP-TTLS via the Print Server Homepage

- The print server is defined as user (with user name and password) on a RADIUS server.




Proceed as follows:



1. *Start the Print Server Homepage.*
 2. *Select **Configuration - Protection**.*
 3. *Select **Authentication**.*
 4. *Select **EAP-TTLS** from the Authentication list.*
 5. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 6. *Select the settings intended to secure the communication in the TLS channel.*
 7. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇨ 103. While configuring the authentication, via **CA certificates - EAP authentication** select the root CA certificate.*
 8. *Click **Save** to confirm.*
- ↩ The settings are saved.

Requirements

Activating EAP-TTLS via InterCon-NetTool


- The InterCon-NetTool is installed on the client, see: ⇨ 15.
- The print server is defined as user (with user name and password) on a RADIUS server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. *Select **Configuration – Protection** from the navigation bar.*
 4. *Select the **Authentication** tab.*
 5. *Select **EAP-TTLS** from the Authentication list.*
 6. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 7. *Select the settings intended to secure the communication in the TLS channel.*
 8. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇨  103. While configuring the authentication, via **CA certificates – EAP authentication** select the root CA certificate.*
 9. *Click **OK** to confirm.*
-  The settings are saved.

12.4 How to Configure PEAP

The PEAP (Protected Extensible Authentication Protocol) validates the identity of devices or users before they gain access to network resources. You can configure the print server for the PEAP network authentication. This makes sure that the print server gets access to protected networks.

In the case of PEAP, an encrypted TLS (Transport Layer Security) channel is established between the print server and the RADIUS server (as is the case for EAP-TTLS, see ⇨  111). Only the RADIUS server authenticates itself using a certificate that was signed by a CA.

The TLS channel is then used to establish another connection that can be protected by means of additional EAP authentication methods (e.g. MSCHAPv2).

Benefits and Purpose

Mode of Operation

What do you want to do?

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. PEAP uses the advantages of TLS and supports various authentication methods, including user passwords and one-time passwords.

- 'Enabling PEAP via Print Server Homepage' ⇒ 114
- 'Enabling PEAP Via InterCon-NetTool' ⇒ 115



The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Requirements

Enabling PEAP via Print Server Homepage

- The print server is defined as user (with user name and password) on a RADIUS server.




Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Configuration - Protection.**
 3. **Select Authentication.**
 4. **Select EAP-PEAP from the Authentication list.**
 5. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 6. *Select the settings intended to secure the communication in the TLS channel.*
 7. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇒ 103. While configuring the authentication, via CA certificates - EAP authentication select the root CA certificate.*
 8. **Click Save to confirm.**
- ↪ The settings are saved.

Requirements

Enabling PEAP Via InterCon-NetTool

- ☑ The InterCon-NetTool is installed on the client, see: ⇨ 15.
- ☑ The print server is defined as user (with user name and password) on a RADIUS server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list. The Properties dialog appears.*
 3. *Select **Configuration – Protection** from the navigation bar.*
 4. *Select the **Authentication** tab.*
 5. *Select **EAP-PEAP** from the Authentication list.*
 6. *Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.*
 7. *Select the settings intended to secure the communication in the TLS channel.*
 8. *To make the connection more secure, you can also install the root CA certificate of the certification authority that has issued the certificate of the authentication server (RADIUS) on the print server; see: 'How to Save CA Certificates in the Print Server' ⇨ 103. While configuring the authentication, via **CA certificates – EAP authentication** select the root CA certificate.*
 9. *Click OK to confirm.*
-  The settings are saved.

Benefits and Purpose

12.5 How to Configure EAP-FAST

EAP-FAST (Flexible Authentication via Secure Tunneling) validates the identity of devices or users before they gain access to network resources. You can configure the print server for the EAP-FAST network authentication. This makes sure that the print server gets access to protected networks.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS ⇨ 111) a channel in order to protect the data transfer. The main difference is that EAP-

FAST does not require certificates for authentication purposes. (The use of certificates is optional.)


PACs (Protected Access Credential) are used to build the channel. PACs are credentials that comprise up to three components.

- A shared secret key that contains the preshared key between the print server and the RADIUS server.
- An opaque part that is provided to the print server and presented to the RADIUS server when the print server wishes to obtain access to network resources.
- Other information that may be useful to the client. (Optional)

EAP-FAST uses two methods to generate PACs:

- The manual delivery mechanism can be every mechanism that the administrator configures and considers to be safe for the network.
- In the case of the automatic delivery, an encrypted channel is established in order to protect the authentication of the print server as well as the delivery of the PACs.

'Enabling EAP-FAST via the Print Server Homepage' ⇨  116

'Enabling EAP-FAST via InterCon-NetTool' ⇨  117



The authentication of print server models with WLAN support is configured via the menu item **Configuration - WLAN**.

Enabling EAP-FAST via the Print Server Homepage

Requirements

- The print server is defined as user (with user name and password) on a RADIUS server.



Proceed as follows:

1. *Start the Print Server Homepage.*
2. *Select **Configuration - Protection**.*
3. *Select **Authentication**.*


What do you want to do?

Requirements

4. Select **EAP-FAST** from the **Authentication** list.
 5. Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.
 6. Select the settings intended to secure the communication in the channel.
 7. Click **Save** to confirm.
- ↪ The settings are saved.

Enabling EAP-FAST via InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- The print server is defined as user (with user name and password) on a RADIUS server.

 Proceed as follows:

1. Start the *InterCon-NetTool*.
 2. Double-click the print server in the device list.
The **Properties** dialog appears.
 3. Select **Configuration – Protection** from the navigation bar.
 4. Select the **Authentication** tab.
 5. Select **EAP-FAST** from the **Authentication** list.
 6. Enter the user name and the password that are used for the configuration of the print server on the RADIUS server.
 7. Select the settings intended to secure the communication in the channel.
 8. Click **OK** to confirm.
- ↪ The settings are saved.

13 Maintenance



A number of maintenance activities can be carried out on the print server. This chapter contains information on securing and resetting the parameter values. You will also learn how to carry out a restart and a device update.

What Information Do You Need?

- 'How to Secure the Print Server Parameters (Backup)' ⇨ 119
- 'How to Reset Parameters to their Default Values' ⇨ 123
- 'How to Perform an Update' ⇨ 127
- 'How to Restart the Print Server' ⇨ 133

13.1 How to Secure the Print Server Parameters (Backup)

All parameter values of the print server (exception: passwords) are saved in the 'parameters' file.

You can save the parameters file as backup copy on your local client. This allows you to get back to a stable configuration status at any time.

You can edit the parameter values of the copied file using a text editor. Afterwards, the configured file can be downloaded to one or more print servers. The parameter values included in the file will be taken over by the device.


What do you want to do?

- 'Saving the Parameters File to the Client via the InterCon-NetTool' ⇨ [119](#)
- 'Editing the Parameters File' ⇨ [121](#)
- 'Downloading the 'Parameters' File to one or more Print Servers using the InterCon-NetTool' ⇨ [121](#)
- 'Load the Parameters onto the Print Server via the Print Server Homepage' ⇨ [122](#)
- 'Resetting Parameters via the Print Server Homepage' ⇨ [124](#)
- 'Resetting Parameters via the InterCon-NetTool' ⇨ [124](#)
- 'Resetting Parameters via an FTP Connection' ⇨ [124](#)
- 'Resetting the Parameters via the Button' ⇨ [125](#)

Saving the Parameters File to the Client via the InterCon-NetTool

Requirements

- The InterCon-NetTool is installed on the client, see: ⇨ [15](#).

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select one or more print servers in the device list.*
3. *Select Actions – Download parameters file an. The Parameter Download dialog appears; see Fig. 7 ⇨ [120](#).*
4. *Select a print server.*

5. Click **Get parameters file**.
The **Save As** dialog appears.
 6. Enter the file name and path.
 7. Click **Save**.
The parameter file is copied and secured.
 8. Repeat 4–7 until you have saved the parameters files from all selected print servers.
- ↩ The parameters are saved.



If you want to change parameters, you can open the file directly in a text editor in order to edit the parameter values; see: ↗ 121.

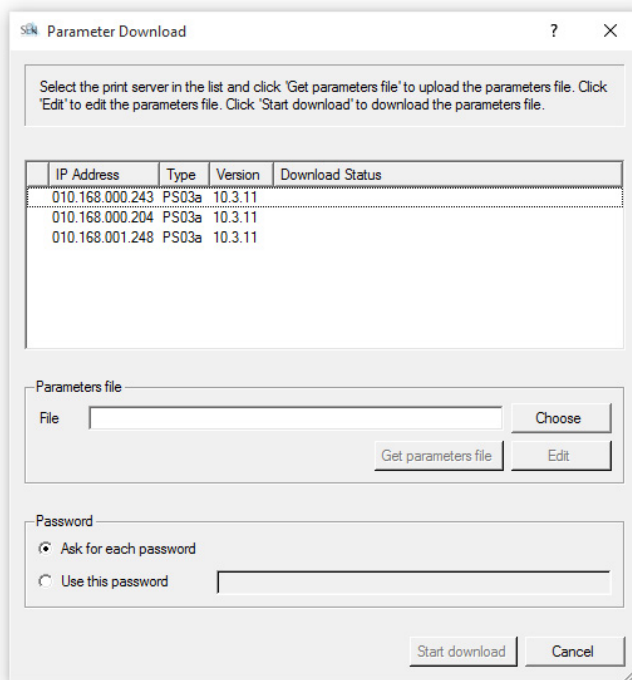


Fig. 7: InterCon-NetTool - Parameter download

Requirements

Editing the Parameters File

Using a text editor, you can edit the parameter values in the parameters file. Via the InterCon-NetTool, you can open the file directly in a text editor. Alternatively you can open the parameters file in a text editor with the usual mechanisms of your operating system.

- ☑ The InterCon-NetTool is installed on the client, see: ⇨ [15](#).
- ☑ The parameters file has been saved on the client; see: ⇨ [119](#).
- ☑ A text editor is installed on the client.



Only change the parameter values. Other changes (layout, etc.) will render the parameters file unusable for the print server.

Proceed as follows:

1. *Click Edit.*
The file is opened in the text editor.
2. *Edit the parameters file. For information on the parameter values, see: 'Parameterliste' ⇨ [162](#).*
3. *Save the parameters file.*
4. *Close the text editor.*
5. *Load the changed parameters file onto a print server.*
 - 'Downloading the 'Parameters' File to one or more Print Servers using the InterCon-NetTool' ⇨ [121](#),
 - 'Load the Parameters onto the Print Server via the Print Server Homepage' ⇨ [122](#).


Downloading the 'Parameters' File to one or more Print Servers using the InterCon-NetTool



When downloading the parameters file to several print servers, the parameter default settings 'IP address,' 'host name', and 'NetBIOS Name' of the respective print server will be maintained. All other settings will be overwritten by those in the parameters file.

Requirements

- ☑ The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select one or more print servers from the device list.*
3. *Select Actions – Download parameters file.*
The Parameter Download dialog appears; see Fig. 7 ⇒ 120.
4. *Click Choose.*
The Parameter Download dialog appears.
5. *Specify the 'parameters' file.*
6. *Click Open.*
7. *Decide on the password option:*
 - *If the print server displayed in the list are not password-protected or protected by different passwords, tick Ask for each password.*
 - *If the print servers are protected by the same password, tick Use this password and enter the password.*
8. *Click Start download.*




By clicking 'Start download', the selected file will be downloaded to all print servers displayed in the list. If you do not want to download the file to all print servers, you must close the dialog and only select the desired print servers from the print server list (see step 2.).

9. *Confirm the security query.*
 10. *Enter the password(s), if necessary.*
- ☞ The parameters file will be loaded onto the print server(s). The parameter values in the file are applied to the print server(s).

Load the Parameters onto the Print Server via the Print Server Homepage

All previous print server settings will be overwritten.

 Proceed as follows:

1. *Start the Print Server Homepage.*

2. *Select Actions – Download Area.*
 3. *Select Parameter Download.*
 4. *Click Browse.*
 5. *Specify the 'parameters' file.*
 6. *Click Open.*
 7. *Click Download.*
 8. *Enter the print server password, if necessary.*
- ↳ The parameter values in the file are applied to the print server.

13.2 How to Reset Parameters to their Default Values

You can reset all print server parameters to their default values (factory default settings). All previously configured parameter values will be deleted in this process. Installed certificates will not be deleted.



If you reset the parameters, the IP address of the print server may change and the connection to the Print Server Homepage may be terminated.

When is Resetting Recommended?

You must reset the parameters, for example, if you want to use the print server in another network by changing the location of the printer. Before this change of location, you should reset the parameters to the default settings to install the print server in another network.

What do you want to do?


- 'Resetting Parameters via the Print Server Homepage' ⇒ 124
- 'Resetting Parameters via the InterCon-NetTool' ⇒ 124
- 'Resetting Parameters via an FTP Connection' ⇒ 124
- 'Resetting the Parameters via the Button' ⇒ 125



By means of the button of the print server operating panel you can reset the parameters without entering the password.

Requirements

Resetting Parameters via the Print Server Homepage


 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Actions – Default Settings.**
3. **Click Default settings.**

 The parameters are reset.

Resetting Parameters via the InterCon-NetTool


The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*
3. **Select Actions – Default Settings from the menu bar.**
4. **Click Finish.**

 The parameters are reset.

Resetting Parameters via an FTP Connection

 Proceed as follows:

1. *Open an FTP connection to the print server:*
Syntax: ftp <IP address>
Example: ftp 192.168.0.123
2. *Enter either the print server password or press the enter key if no password has been assigned.*
3. *Reset the parameters:*
quote SITE RESET
4. *Close the FTP connection:*
quit
5. *Interrupt the power supply of the print server. To do this, disconnect the power supply from the print server and then reconnect it.*

 The parameters are reset.

Resetting the Parameters via the Button

Using the button you can reset the print server's parameter values to their default setting. The reset process can be divided into three phases:

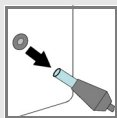
- During phase 1, the device is forced into the reset mode. During the reset mode, the parameters are reset.
- The second phase is the restart of the printer respectively print server.
- The third phase describes the printing of a status page. The reset process can be checked by means of the status page. (Note: A status page cannot be printed via GDI printers.)



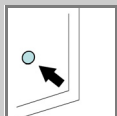
IMPORTANT: The reset mode is indicated by the synchronous blinking of the activity LED (yellow) and the status LED (green) and last for about five intervals.

You must release the button within this time frame, otherwise the device switches to the BIOS mode. If this happens, try the reset again.

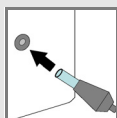
The phases are described in the following: The illustrations may differ slightly from your print server model.

[Phase 1] Reset

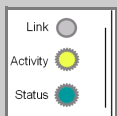
Turn off the print server / interrupt the power supply.*



Press and hold the button.

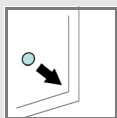


Turn on the print server / establish the power supply.



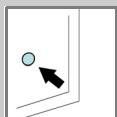
Wait until the activity LED and status LED blink synchronously.

The reset mode has been activated.



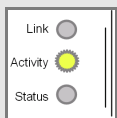
Release the button for a short time (2 seconds at most).

The LEDs blink alternately.

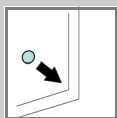


Press and hold the button again.

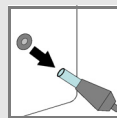
The LEDs blink synchronously.



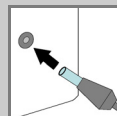
After a few seconds, only the activity LED will blink.



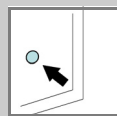
Release the button.

[Phase 2] Restart

Turn off the print server / interrupt the power supply.*



Turn on the print server / establish the power supply.

[Phase 3] Status check

Press the button for a short time.

The status page is printed.

13.3 How to Perform an Update

What Happens during an Update?

You can carry out software and firmware updates on the print server. Updates allow you to benefit from currently developed features.

In the course of an update, the old firmware/software will be overwritten and replaced by the new firmware/software. The parameter default settings of the device remain unchanged.

When is an Update recommended?

You should update your print server if some functions do not work properly and if a new software with new functions or bug fixes has been released by SEH Computertechnik GmbH .

Check the currently installed software and firmware version of your print server. The version number can be found in the device list of the InterCon-NetTool. You can also start the Print Server Homepage and select **Status - General**.

Where do I Find the Update Files?

Current firmware and software files can be downloaded from the SEH Computertechnik GmbH website:

<http://www.seh-technology.com/services/downloads.html>



Every update file has its own 'readme' file. Take note of the information contained in the 'readme' file.

Update possibilities

An update can be carried out manually (standard update) or automatically (dynamic update).

- In the case of a standard update, the update file is downloaded manually from a server or a data medium and saved in the print server.

- With a dynamic update, polling is performed each time the print server is restarted to determine whether, in the meantime, a later version of the update file has been stored on the specified file server. If this is the case, the update file is automatically saved in the print server via FTP.



The dynamic update cannot be used to save an earlier version of the software in the print server. In this case use the standard update.

In order to reduce the amount of administration you can carry out an update on several print servers simultaneously.

What do you want to do?

- 'Standard Update via Print Server Homepage' ⇒ 128
- 'Standard Update via InterCon-NetTool' ⇒ 129
- 'Standard Update via FTP' ⇒ 130
- 'Dynamic Update via Print Server Homepage' ⇒ 130
- 'Dynamic Update via InterCon-NetTool' ⇒ 131
- 'Dynamic Update via FTP' ⇒ 132
- 'Updating Several Print Servers Simultaneously' ⇒ 132

Requirements

Standard Update via Print Server Homepage

- All print jobs are finished.




Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Actions – Download Area.**
 3. **Select Standard Firmware Update.**
 4. **Click Browse.**
 5. *Select the update file.*
 6. **Click Download.**
- ↪ The update is executed. The print server is restarting.

Requirements

Standard Update via InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ 15.
- All print jobs are finished.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print server from the device list.*
 3. *From the menu bar, select Actions – Firmware Update – Standard Update.*
The standard update dialog appears; see . Fig. 8 ⇨ 129.
 4. *Click Choose.*
 5. *Select the update file.*
 6. *Click Start update.*
 7. *Confirm the security query.*
-  The update is executed. The print server is restarting.

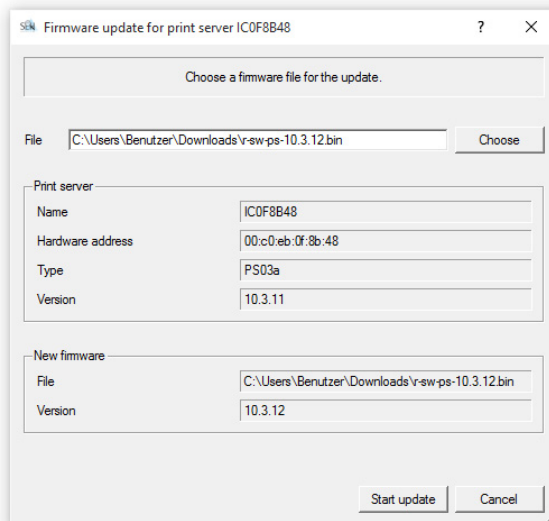



Fig. 8: InterCon-NetTool – Standard update

Requirements

Standard Update via FTP

You can do a standard update on your print server via an FTP connection.

- The print server has a suitable IP configuration, see: ⇒ 7.
- You know the print server's current IP address; see: ⇒ 7.
- All print jobs are finished.

 Proceed as follows:

1. *Change to the directory where the update file is located.*
2. *Open an FTP connection to the print server:*
Syntax: `ftp <IP address of the print server>`
Example: `ftp 192.168.0.123`
3. *Enter an arbitrary user name.*
4. *Enter either the print server password or press the enter key if no password has been assigned.*
5. *Switch to binary mode:*
`bin`
6. *Send the update file to the print server:*
Syntax: `put <update file name> binfile`
Example: `put a-fw-ps-12.bin binfile`
7. *Close the FTP connection:*
`quit`


Dynamic Update via Print Server Homepage

Specify a directory on the file server for automatic (dynamic) updates. The directory contains the current update files. If the print server restarts, it checks if a new update file was put into the directory. If this is the case, the print server will be updated automatically.

Requirements

- All print jobs are finished.
- The update files are in a directory.
- The file server on which the update files are stored either uses the 'anonymous login' or the print server is set up as 'user' on the file server.

Requirements

 Proceed as follows:


1. *Start the Print Server Homepage.*
2. *Select Actions – Download Area.*
3. *Select Dynamic Firmware Update.*
4. *Tick Dynamic Firmware Update.*
5. *In the Update URL box, specify the IP address of the file server on which the new updates files are to be stored.*

Syntax: ftp://<IP address of the file server>/
<software file name>

Example: ftp://192.168.0.100/a-fw-ps-12.bin


(If your system supports name resolution via WINS, DHCP, or DNS, you can enter the name of the file server instead of the IP address of the file server).


Example: ftp://192.168.0.100/a-fw-ps-12.bin

6. *If you use a proxy server, tick Use proxy and enter the IP address of the proxy server.*
 7. *Click Save to confirm.*
-  The settings are saved.


Dynamic Update via InterCon-NetTool

Specify a directory on the file server for automatic (dynamic) updates. The directory contains the current update files. If the print server restarts, it checks if a new update file was put into the directory. If this is the case, the print server will be updated automatically.

- The InterCon-NetTool is installed on the client, see:  15.
- All print jobs are finished.
- The update files are in a directory.
- The file server on which the update files are stored either uses the 'anonymous login' or the print server is set up as 'user' on the file server.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*

3. **Select Actions – Firmware Update – Dynamic Update** from the menu bar.
The Dynamic update for print server dialog appears.
 4. **Tick Dynamic Firmware Update.**
 5. **Specify the IP address of the file server on which the new update files are to be stored.**
Syntax: ftp://<IP address of the file server>/<update file name>
Example: ftp://192.168.0.100/a-fw-ps-12.bin
(If your system supports name resolution via WINS, DHCP, or DNS, you can enter the name of the file server instead of the IP address of the file server).
Example: ftp://192.168.0.100/a-fw-ps-12.bin
 6. **If you use a proxy server, tick Use proxy and enter the IP address of the proxy server.**
 7. **Click OK to confirm.**
-  The settings are saved.

Dynamic Update via FTP



The parameters for a dynamic update can also be configured via FTP. 'Administration via FTP/FTPS-Verbindung' ⇒ 17.

Updating Several Print Servers Simultaneously

The InterCon-NetTool allows you to update more than one print server simultaneously.

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.
- All print jobs are finished.
- All required update files are located in one directory.



Proceed as follows:

1. **Start the InterCon-NetTool.**
2. **Select the print server from the device list.**
3. **Select Actions – Firmware Update** from the menu bar.
The Firmware Update dialog appears.
4. **Click Choose.**


5. *Select the directory in which the update files are located.*
 6. *Click **OK** to confirm.*
 7. *Check whether the right update files are shown in the list. If necessary, change the assignment of the update files to the print servers by right-clicking the print server and choosing a different file.*
 8. *If one single password is used for all print servers, select **Use this password** and enter the password.*
 9. *Click **Start update**.*
 10. *Confirm the security query.*
- ↪ The update is executed. The print servers are restarted.

13.4 How to Restart the Print Server

If the print server is in an undefined state, the it can also be rebooted manually.

- 'Restarting the Print Server using the Printserver Homepage' ⇒ 133
- 'Restarting the Print Server via the InterCon-NetTool' ⇒ 133


Restarting the Print Server using the Printserver Homepage

 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. *Select **Actions – Restart**.*
 3. *Click **Restart Print Server**.*
- ↪ The print server is restarting.

Restarting the Print Server via the InterCon-NetTool

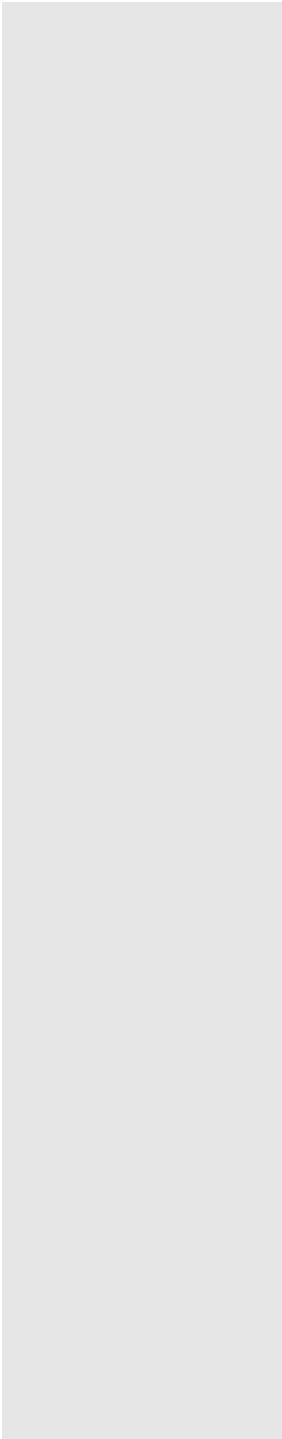
- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Select the print server from the device list.*

What do you want to do?

Requirements

- 
3. *Select Actions – Restart from the menu bar.*
The Restart print server dialog appears.
 4. *Click Finish.*
- ↳ The print server is restarting.

14 Additional Feature – ThinPrint®



Print servers are equipped with a ThinPrint feature. This chapter describes how to use the print server in a ThinPrint environment.

What is ThinPrint®?

ThinPrint® is a software-based technology providing print job compression and bandwidth control for network printing. The data traffic between the print server and the local printer is reduced considerably and networks are taxed less.

Mode of Operation

Print jobs are compressed using the server component **ThinPrint Engine**. The server sends the compressed print data to a device on which a **ThinPrint Client** is implemented, e.g. the print server. The ThinPrint client then decompresses the print data and transfers it to any printer.



The settings described here refer to the client-side (print server). Information about the installation, configuration and administration of the ThinPrint environment can be found in the ThinPrint documentation at <http://www.thinprint.de>.

What do you want to do?

- 'How to Address the Print Server in a ThinPrint Environment' ⇒ 136
- 'How to Define the ThinPrint Port' ⇒ 136
- 'How to Define the Bandwidth' ⇒ 137
- 'How to Use ThinPrint AutoConnect' ⇒ 138
- 'How Does the Print Server Receive Encrypted Data?' ⇒ 140

14.1 How to Address the Print Server in a ThinPrint Environment

Use the following syntax to address the print server in ThinPrint environments:

Syntax:

```
<IP address or host name of the print server>:
<number of the logical printer>#<arbitrary name>
```

Example:

```
192.168.0.123:1#IC0001FF
```

14.2 How to Define the ThinPrint Port


In ThinPrint environments, printing is done to a TCP/IP port via a socket connection. The port number of the print server must be identical to the port number that was defined for the ThinPrint server.

The port 4000 is preset. You can change the port number, if necessary.

What do you want
to do?

- 'Configuring the ThinPrint Port via Print Server Homepage' ⇨ 136
- 'Configuring the ThinPrint Port via InterCon-NetTool' ⇨ 137


Configuring the ThinPrint Port via Print Server Homepage

 Proceed as follows:


1. *Start the Print Server Homepage.*
 2. *Select Configuration – ThinPrint®.*
 3. *Into the ThinPrint® port box, enter the port number.*
 4. *Click Save to confirm.*
- ↪ The setting will be saved.

Requirements**Configuring the ThinPrint Port via InterCon-NetTool**

The InterCon-NetTool is installed on the client, see: [⇒ 15](#).

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list. The Properties dialog appears.*
3. **Select Configuration – ThinPrint®.**
4. *Into the ThinPrint® port box, enter the port number.*
5. *Click OK to confirm.*

 The setting will be saved.

14.3 How to Define the Bandwidth

The bandwidth describes the capacity of a data connection. The bandwidth of the print server is indicated in bit/second (bit/s).

The bandwidth that is needed for print jobs can be limited to a freely definable value for each ThinPrint port (server side). You can further decrease the bandwidth limit on the port of the print server (client side).




Defining a bandwidth value on the print server which is higher than the defined value (server side) will have no effect. In this case, the pre-defined value will be applied.

What do you want to do?

- 'Configuring the Bandwidth via Print Server Homepage' [⇒ 137](#)
- 'Configuring the Bandwidth via InterCon-NetTool' [⇒ 138](#)

Configuring the Bandwidth via Print Server Homepage

 Proceed as follows:


1. *Start the Print Server Homepage.*
2. **Select Configuration – ThinPrint®.**
3. **Tick Bandwidth.**

Requirements

4. *Enter the desired bandwidth (bit/s).*
 5. *Click Save to confirm.*
- ↳ The setting will be saved.

Configuring the Bandwidth via InterCon-NetTool

- The InterCon-NetTool is installed on the client, see: ⇨ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Double-click the print server in the device list.*
The Properties dialog appears.
 3. *Select Configuration – ThinPrint®.*
 4. *Tick Bandwidth.*
 5. *Enter the desired bandwidth (bit/s).*
 6. *Click OK to confirm.*
- ↳ The setting will be saved.

14.4 How to Use ThinPrint AutoConnect

ThinPrint AutoConnect is a tool within the ThinPrint technology for the automatic creation of print objects. The printer objects are created on the basis of defined templates without the need to automatically load the printer drivers.


Printers can be combined in printer groups and printer locations on the basis of so-called printer classes. A name table translation (Dynamic Printer Matrix) simplifies the creation of classes and the assignment of printers.


In the case of several drivers we recommend the assignment of the appropriate printer drivers via the printer class. This assignment can be set up accordingly in the printer configuration on the ThinPrint client.

What do you want to do?

- 'Configuring AutoConnect via Print Server Homepage' ⇨ 139
- 'Configuring AutoConnect via InterCon-NetTool' ⇨ 139

Configuring AutoConnect via Print Server Homepage

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – ThinPrint®.**
3. *Configure the AutoConnect parameters; see: Table 16* ⇨  **139.**
4. *Click Save to confirm.*

⇨ The setting will be saved.


Table 16: ThinPrint AutoConnect parameters


Parameters	Description
ID	The ID clearly identifies the printers for the ThinPrint server.
printer	Defines the printer name. The printer name is purely a description and is used to distinguish the printers.
Class	Printers with compatible drivers can be arranged in one class.
Driver	Specifies the printer driver for the embedded printer.

Requirements

Configuring AutoConnect via InterCon-NetTool

The InterCon-NetTool is installed on the client, see: ⇨  15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Double-click the print server in the device list.*
3. **Select Configuration – ThinPrint®.**
4. *Configure the parameters; see: Table 16* ⇨  **139.**
5. *Click OK to confirm.*

⇨ The setting will be saved.

14.5 How Does the Print Server Receive Encrypted Data?

A secure connection during the transfer of print jobs between the ThinPrint® server and the print server is guaranteed by means of an SSL/TLS encryption.

The ThinPrint server requests a certificate from the print server. By means of this certificate, the ThinPrint server checks whether the print server is authorized to receive the print data.

If an encryption was enabled on the ThinPrint server, you must install a certificate from a corresponding Certification Authority (CA) both on the ThinPrint server and the print server. To authorize the print server to receive encrypted print data, proceed as follows:

- Create a certificate request; see: ⇒ 95.
- Save the requested certificate; see: ⇒ 97.

15 Additional Feature – Internet Protocol Security (IPsec)



To defend against threats against the network, the IPsec protocol provides confidentiality, authenticity and integrity for the IP-based network traffic. The print server can participate in various IPsec procedures. This chapter describes which procedures are supported and how these procedures are configured on the print server.

What is IPsec?

'Internet Protocol Security' (IPsec) is a protocol that provides security mechanisms such as access control, data integrity, encryption and authentication for the communication via IP networks.

What is special about IPsec is its flexibility. You can enable or disable functions according to your needs. When it comes to encryption and authentication, you can freely define the algorithms to be used.

The IPsec security mechanisms are provided by two protocols—the 'Authentication Header' (AH) or 'Encapsulating Security Payload' (ESP). AH will only provide for authentication while ESP will (in addition to authentication) encrypt the IP data packets.

IPsec Policy

IPsec policies are used to assign and handle IP data packets. You can specify several policies. However, only one policy can be active at a time. An IPsec policy is a collection of one or more rules.

IPsec analyzes all IP data packets for addresses, ports, and transport protocols via packet filtering. Based on the rules it is decided how to proceed with the IP data packet. An IPsec policy consists of the following elements:

Table 17: Components of an IPsec policy

Component	Description
Filter list	<p>A filter list contains one or several filters. A filter is the description of</p> <ul style="list-style-type: none"> - IP traffic (IP address / IP address range) and - protocols and services that are used.

Security association**How Does an SA Work?**

Component	Description
Filter action	This is the action to be carried out if a data packet matches the description of a filter. The following actions can be defined: <ul style="list-style-type: none"> - Allow IP data packet, - Block IP data packet, - Forward IP data packets via a 'security association'.
Rule	A rule is composed of a filter list and a filter action. Thus it is specified that a certain action belongs to a certain filter.

If an IP data packet is forwarded via a 'security association', the actual IPsec security will be applied.

A security association (SA) is the establishment of shared security information between two network entities. It serves as a basis for the use of IPsec and can be compared to a tunnel.

The SA specifies which security measures to use for a packet. SAs are established between sender and recipient. The following SA parameters are required:

- authentication method of the participants (pre-shared key or certificate)
- key algorithm to be used for the IPsec connection (see: Table 21 ⇨ 153)
- time after which another authentication is required (optional)
- time after which the IPsec key must be renewed (optional)

When using an SA the tunnel parameters must be defined. When a packet must be sent through a non-existing tunnel (SA), the print server establishes contact with the remote server.

In the so-called 'main mode' the print server sends its suggestions concerning the tunnel parameters. The remote server chooses one suggestion and sends it back.

Alternatively you can choose the 'aggressive mode' that offers almost the same functions but needs fewer packets. (The 'aggressive mode' is less secure and should only be used if the remote IP address is known.)

**Structure and
Procedure**

Afterwards, information for the authentication of the remote server and the agreement about a key (Diffie-Hellman algorithm) will be transferred.

Two different methods are used for authentication purposes.

- authentication via 'Pre-Shared Keys' (PSK) or a
- certificate-based authentication

After the print server and remote server have specified the SA parameters, the IP data packets that are to be encrypted will be sent by the SA together with the ESP protocol (or the AH protocol).

Moreover, 'Internet Key Exchange' (IKE) is used as a protocol for the key exchange or key management together with the 'Internet Security Association and Key Management Protocol' (ISAKMP).

The kernel has two databases for the use of IPsec.

- Security Policy Database (SPD)
The kernel refers to the SPD in order to decide if a particular IP data packet needs to be processed by IPsec or not. The SPD also contains entries that specify which IPsec SA and in what form an IPsec SA is to be used.
- Security Association Database (SAD)
The SAD contains the keys for each IPsec SA.

The illustration shows the cooperation between SPD, SAD, and kernel while using IPsec SA with keys.

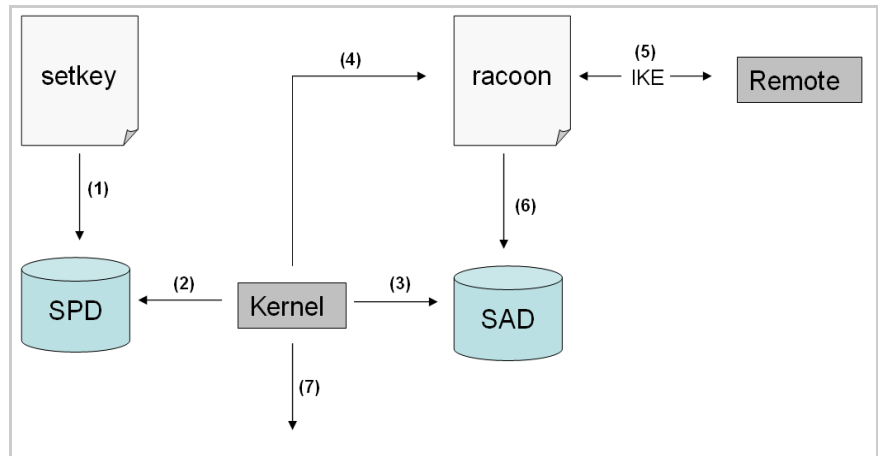


Fig. 9: IPsec procedure

- (1) The administrator defines a policy in the SPD via 'setkey'.
- (2) The kernel refers to the SPD to determine if IPsec can be used for an IP data packet.
- (3) If a key is required for the IPsec-SA, the kernel will get the key from the SAD.
- (4) If the SAD has no key, the kernel sends a request to 'racoon'.
- (5) 'racoon' uses IKE to exchange keys with the remote server.
- (6) 'racoon' writes the key to the SAD.
- (7) The kernel is able to send IPsec data packets.

You can use manual keys or an IKE daemon (e.g. racoon) for authentication purposes. racoon provides the automatic key exchange between two hosts. The setup of a policy in the SPD is required in both cases.

When using manual keys, you must make entries in the SAD in order to provide the encryption method and the keys for a secure communication with other hosts. When using an IKE daemon, the SAs are created automatically.

What is the Task of the Print Server?

The print server offers two ways to implement IPsec policies including SA:

- You can create an IPsec policy via the Print Server Homepage. An input mask assists you in defining the rules.
- Via the Printserver Homepage you can import IPsec policies as ready-made configuration files (racoon/setkey) to the print server.

What Information Do You Need?

IP sec Area only accessible via SSL

Filter



Only one IPsec policy can be active at a time



Please do not operate the print server with a dynamic IP address if you use IPsec.

- 'How to Create IPsec Rules' ⇨ 145
- 'How to Use IPsec Configuration Files' ⇨ 155
- 'How to Define Exceptions' ⇨ 157
- 'How to Enable IPsec Policies' ⇨ 157

The access to the IPsec area on the Printserver Homepage is protected via a secure SSL connection.

URLs that require an SSL/TLS connection start with 'https'. During a so-called 'handshake', the client asks for a certificate via a browser.

If a certificate is unknown to the client, the certificate is not classed as 'trusted'. In this case, you will get an error message. Install the certificate on the client using a browser in order to make the certificate known to the client. For more information, refer to the documentation of your browser and operating system.

15.1 How to Create IPsec Rules

This section describes the creation of IPsec rules via the input mask of the Print Server Homepage.

Rule Structure

IPsec rules are composed of filters and actions.

A filter must be defined to check the data traffic. The filter consists of the following elements:

Action

- **Local IP address**
The local IP address corresponds to the IP address of the print server. The existing IPv4 address of the print server will be used and cannot be changed at this point. IPv6 addresses can be defined via an address template.
- **Remote IP address**
Addresses in the format IPv4 and IPv6 are supported. You can also specify IP address ranges. IP addresses and ranges can be stored in address templates and added to a rule.
- **Services**
Specifies the services that are used by an IP data packet. A service includes the protocol to be used and its port. Several protocols can be summarized in one service template and stored using a freely definable name.

An action determines the measure to be taken if an IP data packet corresponds to the description of a filter. The following actions can be selected:

- Allow all (allow IP data packet)
- Drop all (block IP data packet)
- Use IPsec (forward IP data packet via an SA)

SA

If an IP data packet is forwarded via a 'Security Association' you must specify the SA parameters via an SA template. An SA template contains information about the authentication and the key exchange.

To exchange keys, parameters have been specified in the IKE template.

Rules and Priority

The priority of the rules is defined according to the following criteria.

Exclusivity of IP Addresses

Depending on the number of IP addresses contained in an 'address template' the following priority can be determined:

Rule Numbers

- unique IP address (e. g. 192.168.0.194)
- address ranges (e. g. 192.168.0.194/24 or 0.0.0.0/0)

Depending on the rule number the following priority can be determined:

- Based on their priority the rules are processed from top to bottom.
- If a rule can be applied, the corresponding action will be carried out. All other rules will be neglected.
- If no rule can be applied, the default rule will be used.

Examples**Example 1**

Target:

- Each participant in the company is allowed to print via the printer 'x' without any restrictions.
- Due to large print volumes the 'Sales' department is to be excluded.
- Due to sensitive customer data the 'Support' department will only be allowed to print via IPsec. The SA template 'Level 1' will be used for this purpose.

Implementation concept:

Rule	Active	Address filter	Service filter	Action	SA (Security Association)
1	x	Sales (IP range)	All services	Drop all	---
2	x	Support (IP range)	All services	Require IPsec	Level 1
3		---	---	Allow all	---
4		---	---	Allow all	---
Standard rule		Remote IP address	All services	Allow all	---

Example 2

Target:

- No participant in the company is allowed to print via the printer 'y'.
- The 'Sales' and 'Support' departments will be allowed to print.
- Due to sensitive data the Sales Manager is supposed to print via IPsec. The SA template 'Level 1' will be used for this purpose.
- The printer will be configured via IPsec by the 'Support' department only. The SA template 'Level 2' will be used for this purpose.

Implementation concept:

- All relevant printing services are specified in the 'Printing' service filter.
- All relevant protocols for the administration are specified in the 'Configuring' service filter.


Rule	Active	Address filter	Service filter	Action	SA (Security Association)
1	x	Director (IP)	Printing	Require IPsec	Level 1
2	x	Sales (IP range)	Printing	Allow all	---
3	x	Support (IP range)	Configuring	Require IPsec	Level 2
4	x	Support (IP range)	Printing	Allow all	---
Standard rule		Remote IP address	All services	Drop all	---


What do you want to do?

- 'Creating IPsec Rules' ⇨ 148
- 'Enabling IPsec Rules' ⇨ 149
- 'Defining Address Templates' ⇨ 149
- 'Defining Service Templates' ⇨ 151
- 'Defining SA Templates' ⇨ 152
- 'Defining IKE Templates' ⇨ 153

Creating IPsec Rules

IP data packets can be filtered by address and log information and be assigned to an action. The assignment of filters and filter actions is done via rules.


 Proceed as follows:

1. *Start the Print Server Homepage.*
 2. **Select Configuration – IPsec.**
 3. **Select Edit rules.**
 4. *Define the filters.*
To do this, select the templates to be used in the 'Address filter' and 'Service filter' lists.
 5. *Select the filter action to be used in the 'Action' list.*
 6. *If you have chosen the 'Require IPsec' filter action, you must also select the 'Security Association (SA)' to be used.*
 7. **Click Save.**
-  The settings are saved.

Enabling IPsec Rules

An IPsec policy is composed of several rules. The rules to be used must be enabled so that they can be taken into consideration within the IPsec policy. The activity is controlled by means of the check boxes on the left side of the rules.



Afterwards you must enable the entire IPsec policy for the rules to take effect; see:  157.

Defining Address Templates


Local and remote IP addresses can be defined in the address template. Addresses in the format IPv4 and IPv6 are supported.

3 address templates are implemented by default. You can specify another 5 templates, if required.

The IPv4 address of the print server is always used as the local IPv4 address. The address is not shown in the template.



Please use static IP addresses only.

 Proceed as follows:


1. *Start the Print Server Homepage.*
 2. **Select Configuration – IPsec.**
 3. **Select Edit rules.**
 4. **Select Edit address templates.**
 5. *Define the address template; see: Table 18 ⇨ 150.*
 6. **Click Save to confirm.**
-  The settings are saved.


Table 18: Address Template Parameters

Parameters	Description
Name	Name of the address template <i>You can enter a maximum of 18 characters.</i>
Remote (IPv4)	Specifies remote IPv4 addresses or IPv4 address ranges. Formats/Convention/Example: All IPv4 addresses = 0.0.0.0/0 IPv4 address = 192.168.0.1 IPv4 address range = 192.168.0.1/24 <i>The notation of address ranges is done using the CIDR methodology.</i>
Local (IPv6)	Specifies local IPv6 addresses or IPv6 address ranges. Formats/Convention/Example: All IPv6 addresses = ::/0 IPv6 address = 0:0:0:0:FFFF:a.b.c.d IPv6 address range = 0:0:0:0:FFFF:a.b.c.d/96 <i>The notation of address ranges is done using the CIDR methodology.</i>
Remote (IPv6)	Specifies remote IPv6 addresses or IPv6 address ranges. Formats/Convention/Example: All IPv6 addresses = ::/0 IPv6 address = 0:0:0:0:FFFF:a.b.c.d IPv6 address range = 0:0:0:0:FFFF:a.b.c.d/96 <i>The notation of address ranges is done using the CIDR methodology.</i>

Defining Service Templates

A service includes the protocol to be used and its port. Network activities based on this protocol can be added to the IPsec rule by means of a service template. Several services can be combined in a service template.

The service template 'All services' comprises all protocols and is implemented by default. You can specify another 3 templates, if required.

 Proceed as follows:




1. *Start the Print Server Homepage.*
 2. **Select Configuration – IPsec.**
 3. **Select Edit rules.**
 4. **Select Edit service templates.**
 5. *Define the service template; see: Table 19 → 151.*
 6. **Click Save to confirm.**
-  The settings are saved.

Table 19: Service Template Parameters

Parameters	Description
Name	Name of the service template <i>You can enter a maximum of 16 characters.</i>
All	Comprises all protocols.
ICMP	Internet Control Message Protocol
HTTP	Hypertext Transfer Protocol
SNTP	Simple Network Time Protocol
SNMP	Simple Network Management Protocol
IPP	Internet Printing Protocol
Socket printing	Socket printing
LPR	Line Printer Remote
ThinPrint	ThinPrint enables the transmission of compressed and bandwidth-optimized print jobs within a network.

Defining SA Templates

An SA template contains information about the authentication as well as the key exchange between the print server and the remote server. You can specify up to 4 templates, if required.

 Proceed as follows:




1. *Start the Print Server Homepage.*
 2. **Select Configuration – IPsec.**
 3. *Select Edit rules.*
 4. **Select Edit SA templates.**
 5. *Define the SA template; see: Table 20 →  152.*
 6. *Click Save to confirm.*
-  The settings are saved.


Table 20: SA Template Parameters

Parameters	Description
Name	Name of the IPsec template <i>You can enter a maximum of 16 characters.</i>
Authentication type	Specifies the procedure for the authentication of the remote server. Two procedures are available: - authentication via pre-shared key - authentication via certificates <i>For the installation of certificates on print servers; see: →  89.</i>
Verify certificate	Specifies the type of certificate required for the certificate-based authentication. - <u>Disabled</u> : A self-signed certificate is sufficient for the authentication. (Upon delivery, a self-signed certificate is stored in the print server). - <u>Enabled</u> : A root certificate is required for the authentication.
Pre-Shared Key	Specifies the Pre-Shared Key (PSK). You need the key if the 'Pre-Shared Key' procedure has been selected as 'Authentication type'. <i>You can enter a maximum of 16 characters.</i>
IKE	Specifies the template to be used for the automatic key exchange.

Defining IKE Templates

The IKE template contains the parameters to be used for the automatic key exchange.

The 'IKE Default' template has been implemented by default. You can specify another 3 templates, if required.

 Proceed as follows:



1. *Start the Print Server Homepage.*
 2. **Select Configuration – IPsec.**
 3. **Select Edit rules.**
 4. **Select Edit SA templates.**
 5. **Select Edit IKE templates.**
 6. *Define the IKE template; see: Table 21 ⇨  153.*
 7. *Click Save to confirm.*
-  The settings are saved.

Table 21: IKE Template Parameters

Parameters	Description
Name	Name of the IKE template <i>You can enter a maximum of 16 characters.</i>
- Phase 1 - <i>IKE Phase 1 establishes a secure channel.</i>	
Negotiation	Specifies the procedure for the negotiation of the encryption and authentication. In the 'Main Mode' individual connections will be successively established for the individual steps (key exchange etc.). In the 'Aggressive Mode' individual steps of the Main Mode will be summarized (faster but less secure). You can select several procedures. Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of dynamically generated temporary keys. The keys are used during the negotiation.
Cipher algorithm	Specifies the encryption algorithm to be used during the negotiation.

Parameters	Description
Hash algorithm	Specifies the hash algorithm to be used during the negotiation.
IKE SA lifetime	Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required. (Optional) <i>min. 600 s / max. 4294967295 s</i>
- Phase 2 - <i>IKE phase 2 negotiates the encryption and integrity parameters used to secure the data packet to be transferred.</i>	
Encapsulation type	Specifies how the IP data packet is handled within the SA. The IPsec specification differentiates between the 'Transport Mode' and the 'Tunnel Mode'. - In the Transport Mode the IP data packet is encrypted. However, the IP header will be kept. - In the Tunnel Mode a complete IP data packet will be encapsulated in another packet and be given a new IP header. NOTE: The Tunnel Mode cannot be selected via the selection list on the Printserver Homepage . Use a configuration file (racoon/setkey) instead.
Diffie-Hellman group	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2. (Optional)
Cipher algorithm	Specifies the encryption code for phase 2.
Authentication algorithm	Specifies the hash algorithm for phase 2.
With AH protocol	Specifies the use of the 'Authentication Header' protocol for the protection of the packet integrity and packet authentication. <i>AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.</i>
IPsec SA lifetime	Specifies the duration of the IPsec SA connection in seconds. When the IPsec SA lifetime expires, you have to renew the IPsec key. <i>min. 600 s / max. 4294967295 s</i>

15.2 How to Use IPsec Configuration Files

In order to prepare the print server for the IPsec procedure, you must use the following configuration files for the configuration of SPD and SAD.

- 'setkey.conf' to change, add, or delete entries in SPD and SAD.
- 'racoon.conf' to configure the IKE daemon 'racoon' for the automatic key exchange.

What do you want to do?

- 'Creating IPsec Configuration Files' ⇒ 155
- 'Importing IPsec Configuration Files' ⇒ 156
- 'Importing the Pre-Shared Key' ⇒ 156
- 'Importing Certificates' ⇒ 157

Creating IPsec Configuration Files

When creating the configuration file 'racoon.conf' you must specify the reference to the print server certificates as follows:

Example

```
path certificate "/flash";

remote 192.168.0.1 {
    exchange_mode main;
    certificate_type x509 "cert.pem" "pkey.pem";
    verify_cert on;
    my_identifier asn1dn;
    peers_identifier asn1dn;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm sha1;
        authentication_method rsasig;
        dh_group modp1024;
    }
}

sainfo address 192.168.0.2 any address 192.168.0.1 any {
    pfs_group modp768;
    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
}
```




Detailed information about the creation of configuration files would go beyond the scope of this document. You will find more detailed information on the Internet.

Importing IPsec Configuration Files

You must load the files in the print server so that the values of configuration files 'setkey.conf' or 'racoon.conf' can be applied.

Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – IPsec.**
3. **Select Load files.**
4. **Click Browse.**
5. *Select the configuration file.*
6. **Click Load.**
7. **Click Save to confirm.**

The settings of the configuration file will be saved.

Importing the Pre-Shared Key

If the authentication method 'Pre-Shared Key' is used for an SA (see: Table 20 ⇒ 152) the pre-shared key must be saved in the print server.

Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – IPsec.**
3. **Select Load files.**
4. *Next to 'Preshared keys file' click Browse.*
5. *Select the file.*
6. **Click Load.**
7. **Click Save to confirm.**

The pre-shared key is loaded.


Importing Certificates

If an authentication via certificates is used for an SA (see: Table 20 ⇨ 152), you must save certificates in the print server. To save certificates; see: ⇨ 89.


15.3 How to Define Exceptions

Network activities based on the protocols SLP, DHCP, Bonjour, FTP, and NetBIOS can be excluded from the filtering by the IPsec policy.

This ensures that specified network activities are permanently allowed and are not blocked by IPsec.

 Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – IPsec.**
3. **Select Edit rules.**
4. *Enable the relevant protocols under 'IPsec exceptions'.*
5. *Click Save to confirm.*

 The settings are saved.



If all FTP network activities are allowed (FTP = on), you must specify the 'Allow all' action in the default rule.

15.4 How to Enable IPsec Policies

After you have created IPsec policies via input mask or via configuration files and implemented them on the print server, you can enable a policy.

We recommend using the test mode to access the device in case of a misconfiguration. In the test mode, IPsec remains active until the hard reboot of the device. IPsec is disabled after the hard reboot.

Test Mode



The 'test mode' option is activated by default. After a successful test, you must deactivate the test mode so that the access protection remains permanently active.



Proceed as follows:

1. *Start the Print Server Homepage.*
2. **Select Configuration – IPsec.**
3. *Specify the IPsec policy to be used.*
4. **Use configured rules**
(use policy from the manually configured rules)
5. **Use configuration files**
(use policy of the loaded configuration files)
6. *Make sure that the Test mode is enabled.*
7. *Tick IPsec.*
8. *Click Save to confirm.*
The setting will be saved. IPsec is enabled until the next hard reboot.
9. *Check the access to the device.*



If you can no longer access the device, initiate a hard reboot of the device and modify the IPsec policy.

10. *Clear Test mode.*
 11. *Click Save to confirm.*
- ↪ IP traffic will be allowed based on the rules defined in the IPsec policy.

16 Appendix



The appendix contains a glossary, the parameter list, and the index lists of this document.

What Information Do You Need?

- 'Glossary' ⇨ 159
- 'Parameter List' ⇨ 162
- 'Troubleshooting' ⇨ 193
- 'Abbildungsverzeichnis' ⇨ 198
- 'Index' ⇨ 199

16.1 Glossary

This glossary contains information about manufacturer-specific software solutions and terms from the world of network technology.

What Information Do You Need?

Manufacturer-Specific Software Solutions

- 'InterCon-NetTool' ⇨ 160

Network Technology

- 'Default Name' ⇨ 160
- 'Gateway' ⇨ 160
- 'Hardware Address' ⇨ 160
- 'Host Name' ⇨ 160
- 'IP Address' ⇨ 160
- 'MAC Address' ⇨ 161
- 'Subnet Mask' ⇨ 161
- 'Print Server Name' ⇨ 161
- 'TCP/IP Port' ⇨ 161

Default Name

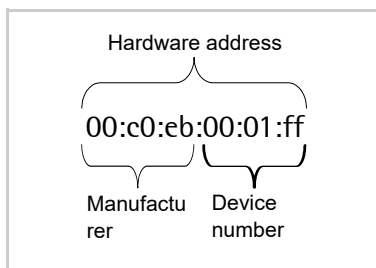
See: 'Print Server Name' ⇒ 161.

Gateway

Using a gateway, you can address IP addresses from other networks. If you wish to use a gateway, you can configure the relevant parameter via the Print Server Homepage or the InterCon-NetTool.

Hardware Address

The print server is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the MAC or Ethernet address. The manufacturer has defined this address in the hardware of the device. The address consists of 12 hexadecimal numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device.



The hardware address is found on the housing of the print server, on the Print Server Homepage, in the InterCon-NetTool, or on the status page.

The use of separators within the hardware address depends on the platform. In Windows '-' are used.

Host Name

The host name is an alias for an IP address. The host name uniquely identifies the print server in the network and makes it easier to remember.

InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices within a predefined network.

IP Address

The IP address is a unique address for every node in your network, i.e., an IP address may appear only once in your local network. The address must be saved in the print server to make sure that it can be addressed within the network.

MAC Address

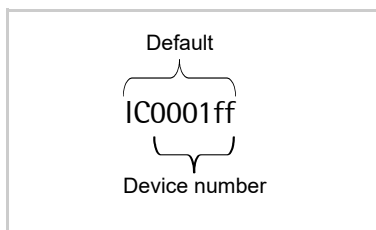
See: 'Hardware Address' ⇒ 160.

Subnet Mask

With the help of the subnet mask, large networks can be split up into subnetworks. In this case, the user IDs of the IP addresses are assigned to the various subnetworks. The print server is configured not to use subnetworks by default. If you wish to use a gateway, you can configure the relevant parameter via the Print Server Homepage or the InterCon-NetTool.

Print Server Name

The print server name (default name) is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of its hardware address.



The default name can be found on the Printserver Homepage or in the InterCon-NetTool.

TCP/IP Port

During the transfer of files between two computers, addressing with the IP address alone is generally not sufficient. In addition to the IP address, a port number (TCP/IP port) is used. This number defines the computer memory area that is reserved for a specific communications connection. The combination of an IP address and a port number is unique for every communications connection and is defined as a socket.

TCP/IP Ports and Logical Printers

The TCP/IP port corresponds to that of the logical printers. The following TCP/IP ports are preset in your print server via the logical printers.

Logical Printer	1	2	3	4	5	6	7	8
TCP/IP Port	9100	9101	9102	9103	9104	9105	9106	9107

**What Information
Do You Need?**

16.2 Parameter List

This chapter gives an overview of all available print server parameters. The parameter list gives details about the functions and values of the individual parameters.

- 'Parameter List - IPv4' ⇨ 163
- 'Parameter List - IPv6' ⇨ 164
- 'Parameter List - Network Speed' ⇨ 165
- 'Parameter List - HTTP' ⇨ 165
- 'Parameter List - NetBIOS/WINS' ⇨ 165
- 'Parameter List - DNS' ⇨ 167
- 'Parameter List - Bonjour' ⇨ 167
- 'Parameter List - POP3' ⇨ 168
- 'Parameter List - SMTP' ⇨ 169
- 'Parameter List - WLAN' ⇨ 170
- 'Parameter List - Device Settings' ⇨ 172
- 'Parameter List - Device Time' ⇨ 172
- 'Parameter List - Print Server Status Information' ⇨ 173
- 'Parameter List - Print jobs and data' ⇨ 173
- 'Parameter List - Port Settings' ⇨ 174
- 'Parameter List - Logical Printers' ⇨ 175
- 'Parameter List - Printer Notifications' ⇨ 178
- 'Parameter List - Security' ⇨ 180
- 'Parameter List - Network Authentication' ⇨ 181
- 'Parameter List - IPsec' ⇨ 182
- 'Parameter List - Dynamic Update' ⇨ 191
- 'Parameter List - ThinPrint®' ⇨ 191



To view the current parameter values of your print server, see: ⇨ 118.

Table 22: Parameter List - IPv4

Parameters	Value	Default	Description
ip_addr [IP address]	valid IP address	169.254. 0.0/16	Defines the IP address of the print server.
ip_mask [Subnet mask]	valid IP address	255.255. 0.0	Defines the subnet mask of the print server.
ip_gate [Gateway]	valid IP address	0.0.0.0	Defines the gateway address of the print server.
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_zconf [ZeroConf]	on/off	on	Enables/disables the ZeroConf (Zero Configuration Networking) protocol.
ip_set_by [IP address]	0–12 [1–2 characters; 0–9] <i>0 = Unknown</i> <i>1 = SNMP (NetTool)</i> <i>2 = BOOTP</i> <i>3 = DHCP</i> <i>4 = PING</i> <i>5 = not defined</i> <i>6 = ZeroConf</i> <i>7 = Parameters file</i> <i>8 = not defined</i> <i>9 = not defined</i> <i>10 = not defined</i> <i>11 = not defined</i> <i>12 = HTTP website</i>		Shows the method used for the IP address assignment.
ip_auto_gate [Multicast router as gateway]	on/off	on	Enables/disables the automatic entry of a found multicast router as gateway address. <i>If disabled, the gateway address has to be entered manually.</i>
sys_name [Host name]	max. 64 characters [a–z, A–Z, 0–9]	[Default name]	Defines the host name of the print server.
sys_contact [Contact person]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the contact person.

Parameters	Value	Default	Description
sys_location [Location]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the device location.

Table 23: Parameter List - IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the print server.
ipv6_addr [IPv6 address]	n:n:n:n:n:n	::	Defines a print server IPv6 unicast address assigned manually in the format n:n:n:n:n:n. <i>Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.</i>
ipv6_gate [Router]	n:n:n:n:n:n	::	Defines the IPv6 unicast address of the router. The print server sends its 'Router Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0–64 [1-2 characters; 0-9]	64	Defines the length of the subnet prefix for the IPv6 address. <i>Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/</i>
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the print server.

Table 24: Parameter List - Network Speed

Parameters	Value	Default	Description
eth_conf [Ethernet settings]	0–5 [1 character; 0–5] <i>0 = automatic</i> <i>1 = 10BaseT/FL half-duplex</i> <i>2 = 10BaseT/FL full- duplex</i> <i>3 = H100BaseFX/TX half-duplex</i> <i>4 = 100BaseFX/TX full duplex</i> <i>5 = 1000BaseT/SX</i>	0	Defines the network speed of the print server. <i>'Auto' means that the network speed is recognized automatically. If the speed is set manually, it must be match that of the other network devices.</i>

Table 25: Parameter List - HTTP

Parameters	Value	Default	Description
http [HTTP]	on/off	on	Enables/disables the HTTP protocol on the print server. <u>Note:</u> If the HTTP protocol is disabled, functions that are based on the protocol will not be available (e.g. the Print Server Homepage cannot be started).

Table 26: Parameter List - NetBIOS/WINS

Parameters	Value	Default	Description
netbios [NetBIOS]	on/off	on	Enables/disables peer-to-peer printing.
netbios_name [NetBIOS-Name]	max. 15 characters [a–z, A–Z, 0–9]	[Default name]	Defines the print server name which appears in the relevant workgroup or domain.
netbios_domain [NetBIOS Domain]	max. 15 characters [a–z, A–Z, 0–9]	[Default name]	Defines the name of an existing workgroup or domain.
netbios_time [NetBIOS refresh every]	0–9999 [1-4 characters; 0-9]	5	Defines the time interval (in minutes) after which the NetBIOS parameters will be refreshed.

Parameters	Value	Default	Description
wins [WINS registration]	on/off	on	Enables/disables the WINS registration.
wins_dhcp [WINS via DHCP]	on/off	on	Enables/disables the automatic entry of the IP address of a WINS server via DHCP. <i>If the option is enabled, the IP address of the WINS server is entered via DHCP. If the option is disabled, you can enter the IP address of the WINS server manually.</i>
wins_primary [Primary WINS server]	valid IP address		Defines the IP address of the primary WINS server.
wins_secondary [Secondary DNS server]	valid IP address		Defines the IP address of the secondary WINS server. <i>The secondary WINS server is used if the primary WINS server is not available.</i>

Table 27: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_domain [Domain name]	max. 255 characters [a–z, A–Z, 0–9]	[blank]	Defines the domain name of an existing DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. <i>The secondary DNS server is used if the primary DNS server is not available.</i>

Table 28: Parameter List - Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
pp*_rdzv_name [Bonjour name]	max. 63 characters [a–z, A–Z, 0–9]	[blank]	Defines the Bonjour name of the print server.

* Port number of the print server (e.g. LPT 1–3, COM1 or USB 1–5)

Table 29: Parameter List - POP3

Parameters	Value	Default	Description
nf_pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.
nf_pop3_srv [Server name]	max. 255 characters	[blank]	Defines the POP3 server via the IP address or the host name. <i>The host name can only be used if a DNS server was configured beforehand.</i>
nf_pop3_port [Server port]	1–65535 [1–5 characters; 0–9]	110	Defines the port of the POP3 server used by the print server for receiving emails. <i>When using SSL/TLS, enter 995 as port number.</i>
nf_pop3_user [User name]	max. 255 characters	[Default name]	Defines the name used by the print server to log on to the POP3 server.
nf_pop3_pwd [Password]	max. 255 characters	[blank]	Defines the password used by the print server to log on to the POP3 server.
nf_pop3_secure [Security]	0–2 [1 character; 0–2] <i>0 = off (no security) 1 = APOP 2 = SSL/TLS</i>	0	Defines an authentication method.
nf_pop3_poll [Check mail every]	0–9999 [1–4 characters; 0–9]	1	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
nf_pop3_limit [Ignore mail exceeding]	0–9999 [1–4 characters; 0–9] <i>0 = unlimited</i>	0	Defines the maximum email size (in Kbyte) to be accepted by the print server.
nf_pop3_mdel [Delete read messages]	on/off	on	Enables/disables the automatic deletion of read emails on the POP3 server.

Table 30: Parameter List - SMTP

Parameters	Value	Default	Description
nf_smtp_srv [Server name]	max. 255 characters	[blank]	Defines the SMTP server via the IP address or the host name. <i>The host name can only be used if a DNS server was configured beforehand.</i>
nf_smtp_port [Server port]	1–65535 [1–5 characters; 0–9]	25	Defines the port number used by the print server to send emails to the SMTP server.
nf_smtp_user [User name]	max. 255 characters	[blank]	Defines the user name used by the print server to log on to the SMTP server.
nf_smtp_pwd [Password]	max. 255 characters	[blank]	Defines the password used by the print server to log on to the SMTP server.
nf_smtp_ssl [TLS]	on/off	off	Enables/disables TLS. <i>The TLS protocol serves to encrypt the transmission between the print server and the SMTP server.</i>
nf_smtp_sndr [Sender name]	max. 255 characters	[Default name]	Defines the email address used by the print server to send emails. Note: Very often the name of the sender and the user name are identical.
nf_smtp_sign [Signature]	max. 128 characters	[Default-Name\r\nSerial: <serial number>\r\nIpAddress: <[IP address]>]	Defines the signature to be contained in an email generated by the print server.
nf_smtp_asp3 [Use POP3 settings]	on/off	off	Takes over the parameters 'User name' and 'Password' from the POP3 settings to log on to the SMTP server.

Table 31: Parameter List - WLAN

Parameters	Value	Default	Description
wifi_mode [Mode]	1–3 [1 characters; 1–3] <i>1 = Infrastructure mode</i> <i>2 = Auto</i> <i>3= Ad-hoc modus</i>	3	Defines the communication mode. <i>The communication mode defines the network structure in which the print server will be installed.</i>
wifi_name [SSID]	max. 64 characters [a–z, A–Z, 0–9, _, -]	SEH	Defines the SSID. <i>The ID of a wireless network is referred to as SSID (Service Set Identifier). Each wireless LAN has a configurable SSID in order to clearly identify the wireless network.</i>
wifi_channel [Channel]	1–13 [1 characters; 0–9] (country-specific – EU only)	3	Defines the channel (frequency range) on which the entire data communication will be transmitted. <i>The channel should be changed if interferences emerge.</i> Keep yourself informed about national provisions regarding the use of WLAN products and only use authorized channels.
wifi_roaming [Roaming]	on/off	off	Enables/disables the use of roaming. <i>Roaming refers to the 'moving' of one radio cell to the next. The print server will use the access point that has the strongest signal. If the print server moves towards the sphere of another access point, the UTN server switches automatically and without loss of connection to the next radio cell.</i>

Parameters	Value	Default	Description
wifi_dbm2roam [dBm]	1–999 [1–3 characters; 0–9]	65	Defines the roaming threshold in -dbm. If the WLAN signal strength exceeds the threshold, the print server searches for a stronger WLAN signal and may switch into a WLAN with better signal strength. This parameter can only be configured in the 'Infrastructure' mode.
wifi_encrypt [Encryption]	0–9 [1 characters; 0–9] <i>0 = none</i> <i>1 = WEP (open system)</i> <i>2 = WEP (shared key)</i> <i>3 = WPA (TKIP)</i> <i>4 = WPA (AES)</i> <i>5 = WPA2 (TKIP)</i> <i>6 = WPA2 (AES)</i> <i>7 = WPA (AES/TKIP)"</i> <i>8 = "WPA2 (AES/TKIP)"</i> <i>9 = WPA (auto)</i>	0	Defines the encryption method to be used to protect the access to the WLAN.
wifi_keyid [WEP key used]	0–4 [1 characters; 0–4] <i>0 = none</i> <i>1 = wifi_wepkey</i> <i>2 = wifi_wepkey2</i> <i>3 = wifi_wepkey3</i> <i>4 = wifi_wepkey4</i>	1	Defines the WEP key to be used.
wifi_wepkey ~ wifi_wepkey4 [WEP Key]	The max. number of characters depends on the mode selected: - 64 ASCII = 5 - 64 HEX = 10 - 128 ASCII = 13 - 128 HEX = 26 <i>You can enter the following characters:</i> <i>- for HEX = 0–9, a–f, A–F</i> <i>- for ASCII = 0–9, a–z, bA–Z</i>	[blank]	Defines the WEP key used.

Parameters	Value	Default	Description
wifi_psk [PSK]	8–63 characters	[blank]	Defines the Pre Shared Key (PSK) for Wi-Fi Protected Access (WPA).

Table 32: Parameter List - Device Settings

Parameters	Value	Default	Description
language [Print server language]	en, de, fr, es, it, pt, jp, cn, zh, kr	en	Defines the language of the print server. <i>en = English</i> <i>de = German</i> <i>fr = French</i> <i>es = Spanish</i> <i>it = Italian</i> <i>pt = Portuguese</i> <i>jp = Japanese</i> <i>cn = Chinese, simplified</i> <i>zh = Chinese, traditional</i> <i>kr = Korean</i>
sys_descr [Description]	max. 128 characters [a–z, A–Z, 0–9]	[blank]	Freely definable description of the contact person.
info_txt [Dealer]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Freely definable name of a dealer or supplier.
info_url [Dealer URL]	max. 64 characters [a–z, A–Z, 0–9, _, -, .]	[blank]	Freely definable URL of a dealer or supplier.

Table 33: Parameter List - Device Time

Parameters	Value	Default	Description
sntp [SNTP]	on/off	on	Enables/disables the use of a time server (SNTP).
sntp_server [Time server]	max. 255 characters [a–z, A–Z, 0–9, _, -, .]	[blank]	Defines a time server via the IP address or the domain name. <i>The host name can only be used if a DNS server was configured beforehand.</i>

Parameters	Value	Default	Description
time_zone [Time zone]	UTC, GMT, EST, EDT, CST,CDT, MST, MDT, PST, PDT, etc.	WET/WE ST (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time.

Table 34: Parameter List – Print Server Status Information

Parameters	Value	Default	Description
sp_mode [Status page mode]	Auto ASCII PostScript DATAMAX Citizen-Z	Auto	Defines the data format in which the status page is printed. <i>The data formats ASCII, PostScript, DATAMAX (label printer), and Citizen-Z (label printer) are available. The preset 'Auto' mode automatically uses the appropriate data format.</i>

Table 35: Parameter List – Print jobs and data

Parameters	Value	Default	Description
job_rcvtimeout [Job receive timeout]	1–9999 [4 characters, 0–9] <i>0 = no timeout</i>	0	Defines the time (seconds) after which the connection to the spooler is closed if no print job is sent to the print server. <i>If the value is set to 0, this function is disabled. If you want to use the timeout option, we recommend using the value '120'.</i>

Table 36: Parameter List - Port Settings

Parameters	Value	Default	Description
pp*_1284_4 [1284.4 / MLC]	on/off	off	Enables/disables the 1284.4/MLC protocol. <i>You can use 1284.4/MLC to obtain enhanced printer status information.</i>
pp*_pjl [PJL]	on/off	off	Enables/disables the PjL (Print Job Language) compatibility. <i>Printers supporting PjL forward enhanced printer information to the print server, if the parameter is enabled.</i>
pp*_ecp [ECP mode]	on/off	off	Enables/disables the ECP mode. <i>The ECP mode (Enhanced Capabilities Port) can be used for quick and compressed data transfer.</i>
pp*_fast [Fast mode]	on/off	on	Enables/disables the fast mode. <i>Using the fast mode, the print server speed can be increased. With older printer models, it is recommended to disable the fast mode.</i>
pp*_port_mode [Port mode]	0–2 [1 character; 0–2] <i>0 = unidirectional 1 = bidirectional 2 = Konica Minolta GDI support</i>	0	Specifies the communication mode between the print server and the printer.
pp4_baudrate [Baud rate]	150, 300, 600, 1200, 1800, 2400, 3600, 4800, 7200, 9600, 19200, 38400, 57600, 115200	9600	Specifies the baud rate for data transfer.
pp4_parity [Parity]	none even odd	none	Specifies the parity bit for the detection of incorrectly transmitted bit sequences (parity check). <i>none = no parity check even = even parity check odd = odd parity check</i>

Parameters	Value	Default	Description
pp4_databits [Data bits]	5–8 [1 characters; 0–9]	8	Specifies how many data bits will be transferred in one data packet.
pp4_stopbits [Stop bits]	1–2 [1 characters; 1–2]	1	Defines the stop bit. <i>Stop bits mark the end of a data transfer unit and allow the recipient of a data transfer to synchronize the data flow.</i>
pp4_flowcontrol [Flow control]	none xon dsr both	xon	Defines the handshake procedure to control the data flow between print server and printer. <i>none = handshake is disabled</i> <i>xon = software handshake is enabled</i> <i>dsr = hardware handshake is enabled</i> <i>both = software and hardware handshake are enabled</i>

* Port number of the print server (e.g. LPT 1–3, COM1 or USB 1–5)

Table 37: Parameter List - Logical Printers

Parameters	Value	Default	Description
lp1_prt_port ~ lp8_prt_port [Printer port]	depends on the print server model	lp1_prt_port = 1 lp2_prt_port = 2 lp3_prt_port = 3 lp4_prt_port = 4 lp5_prt_port = 1 lp6_prt_port = 1 lp7_prt_port = 1 lp8_prt_port = 1	Defines the port used by the logical printer for printing. Note: This parameter is only available for print server models with several physical printer ports.

Parameters	Value	Default	Description
lp1_tcp_port ~ lp8_tcp_port [TCP/IP port]	0–9999 [1–4 characters; 0–9]	9100 9101 ~ 9108	Defines the TCP/IP port of the logical printer.
lp1_mode ~ lp8_mode [Banner page mode]	ASCII PostScript	ASCII	Defines the format in which the banner page is printed.
lp1_ascii_ps ~ lp8_ascii_ps [ASCII/PostScript]	on/off	off	Enables/disables the conversion of ASCII into PostScript data.
lp1_hexdump ~ lp8_hexdump [Hex dump mode]	on/off	off	Enables/disables the hex dump mode. <i>The hex dump mode is used to search for errors in print data.</i>
lp1_binary_ps ~ lp8_binary_ps [Binary PostScript]	on/off	off	Enables/disables the printing of binary PostScript files. <i>Enable this option if binary PostScript files are to be printed in heterogeneous networks.</i>
lp1_job_start ~ lp8_job_start [Job start]	max. 256 characters	[blank]	Defines a start sequence. <i>Depending on the application, you might have to configure the logical printer. For further information; see: ↪ 68.</i>
lp1_job_end ~ lp8_job_end [Job end]	max. 256 characters	[blank]	Defines an end sequence. <i>Depending on the application, you might have to configure the logical printer. For further information; see: ↪ 68.</i>
lp1_search ~ lp8_search [Search]	max. 256 characters [no wildcard or truncations]	[blank]	Defines a string which is searched for in the data sent to the print server. <i>Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings.</i>

Parameters	Value	Default	Description
lp1_replace ~ lp8_replace [Replace]	max. 256 characters [no wildcard or truncations]	[blank]	Defines the string which is replaced in the data sent to the print server. <i>Using 'Find' and 'Replace,' you can look for strings in the data sent to the print server and replace them with new strings.</i>
lp1_crf ~ lp8_crf [CR + LF]	on/off	off	Enables/disables the conversion from line feed (LF) to carriage return with line feed (LF+CR).
lp1_banner ~ lp8_banner [Banner page]	on/off	off	Enables/disables the printing of a banner page if the LPD protocol is used.

Table 38: Parameter List - Printer Notifications

Parameters	Value	Default	Description
nf_mail_pr1 nf_mail_pr2 [Email active]	on/off	off	Enables/disables the email notification for recipient 1 or 2.
nf_mail_addr1 nf_mail_addr2 [Email recipient]	valid email address	[blank]	Defines the email address of the recipient for notifications.
nf_mAccHist1 nf_mAccHist2 [Job History]	on/off	off	Enables/disables the sending of emails containing information on how many prints jobs were handled by the print server to recipient 1 or 2.
nf_mAccHistTime1 nf_mAccHistTime2 [time interval]	0–9999 [1–4 characters; 0–9]	0	Defines the time interval (in hours) with which an email containing information on how many prints jobs were handled by the print server (job history) is sent.
nf_mAccHistCnt1 nf_mAccHistCnt2 [Jobs]	1–60 [1–2 characters; 0–9]	60	Defines the number of print jobs after which an email containing information on how many prints jobs were handled by the print server (job history) is sent to recipient 1 or 2.
nf*_mAccPCnt1 nf*_mAccPCnt2 [Page counter]	on/off	off	Enables/disables the sending of emails containing the number of pages printed by the print server to recipient 1 or 2.
nf*_mAccPCntTi me1 nf*_mAccPCntTi me2 [time interval]	0–9999 [1–4 characters; 0–9]	0	Defines the time interval (in hours) with which an email containing information on how many pages were printed by the printer (page counter) is sent to recipient 1 or 2.
nf*_mAccPCntCnt1 nf*_mAccPCntCnt2 [page interval]	0–9999 [1–4 characters; 0–9]	0	Defines the number of pages after which an email containing information on how many pages were printed by the printer (page counter) is sent to recipient 1 or 2.

Parameters	Value	Default	Description
nf*_mail_mask1 nf*_mail_mask2 [Printer error]	0 = none 1 = paper jam 2 = Paper empty 4 = toner low 8 = printer open 16 = toner empty 32 = cassette not ready 64 = warming up 128 = offline 256 = engine error 512 = no select 1024 = paper low 16384 = call customer service 32768 = miscellaneous error	0	Defines the printer errors of which recipient 1 or 2 is informed by email. <i>The email contains information about the printer error. Each code represents a message. By defining more than one code, several printer errors can be indicated at once.</i> Note: Not all print server models support all printer error messages.
nf_trap_ip1 nf_trap_ip2 [IP address]	valid IP address	[blank]	Defines the SNMP trap address of the recipient.
nf_trap_com1 nf_trap_com2 [Trap community]	max. 15 characters [a–z, A–Z, 0–9]	[blank]	Defines the SNMP trap community of the recipient.
nf_trap_aut1 nf_trap_aut2 [Authentication traps]	on/off	off	Enables/disables the sending of traps containing authentication information.
nf_trap_pr1 nf_trap_pr2 [Printer traps]	on/off	off	Enables/disables the sending of traps for selected printer errors (⇒ 180) for recipient 1 or 2.

Parameters	Value	Default	Description
nf*_trap_mask1	0 = none	0	Defines the printer errors of which recipient 1 or 2 is informed by a trap. <i>A trap contains information about the printer error. Each code represents a message. By defining more than one code, several printer errors can be indicated at once.</i> <u>Note:</u> Not all print server models support all printer error messages.
nf*_trap_mask2	1 = paper jam		
[Printer error]	2 = Paper empty		
	4 = toner low		
	8 = printer open		
	16 = toner empty		
	32 = cassette not ready		
	64 = warming up		
	28 = offline		
	256 = engine error		
	512 = no select		
	124 = paper low		
	16384 = call customer service		
	32768 = miscellaneous error		

* Port number of the print server (e.g. LPT 1–3, COM1 or USB 1–5)

Table 39: Parameter List - Security

Parameters	Value	Default	Description
passwd [Password]	max. 16 characters [a–z, A–Z, 0–9]	[blank]	Defines the password that is needed to authorize print server parameter changes.
access_control [Access control]	on/off	off	Enables/disables the password demand for seeing print server parameters. <i>This parameter only makes sense if a password was set at an earlier stage; see above.</i>


Parameters	Value	Default	Description
ip1_sender ~ ip8_sender [IP sender]	max. 255 characters [The use of wildcards (*) is possible to authorize subnetworks, for example.]	[blank]	Defines the IP address or host name of the client that is authorized to address the print server in the network.  Once an IP sender has been defined, all undefined clients lose their authorization.

Table 40: Parameter List - Network Authentication

Parameters	Value	Default	Description
eap_auth_type [Authentication]	1–7 [1 characters; 1–7] <i>Print Server without WLAN:</i> 1 = not defined 2 = not defined 3 = EAP-MD5 4 = EAP-TLS 5 = EAP-TTLS 6 = EAP-PEAP 7 = EAP-FAST <i>Print Server with WLAN:</i> 1 = Open System 2 = Shared Key 3 = EAP-MD5/ LEAP 4 = EAP-TLS 5 = EAP-TTLS 6 = EAP-PEAP 7 = EAP-FAST	1	Defines the authentication method that is used to identify devices or users in the network.
eap_auth_name [User name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the name of the print server as saved in the authentication server (RADIUS).
eap_auth_pwd [Password]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the password of the print server as saved in the authentication server (RADIUS).

Parameters	Value	Default	Description
eap_auth_extern [EAP- (PEAP/FAST) options]	0–5 [1 characters; 0–5] <i>0 = none</i> <i>1 = PEAPLABEL0</i> <i>2 = PEAPLABEL1</i> <i>3 = PEAPVER0</i> <i>4 = PEAPVER1</i> <i>5 = FAST INLINE PROVISIONING</i>	0	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.
eap_auth_intern [Inner Authentication]	0–8 [1 characters; 0–8] <i>0 = none</i> <i>1 = MS-CHAP</i> <i>2 = MS-CHAPv2</i> <i>3 = PAP</i> <i>4 = CHAP</i> <i>5 = EAP-MD5</i> <i>6 = EAP-MS-CHAP</i> <i>7 = EAP-MS- CHAPv2</i> <i>8 = EAP-TLS</i>	0	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.
eap_auth_anony- mous_name [Anonymous name]	max. 64 characters [a–z, A–Z, 0–9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.

Table 41: Parameter List - IPsec

Parameters	Value	Default	Description
ipsec [IPsec]	on/off	off	Enables/disables the use of IPsec.
ipsec_testmode [Test mode]	on/off	on	Enables/disables the IPsec test mode. <i>We recommend using the test mode to access the device in case of a misconfiguration. In the test mode, IPsec remains active until the hard reboot of the device. IPsec is disabled after the hard reboot.</i>

Parameters	Value	Default	Description
ipsec_config	0–1 [1 characters; 0–1] <i>0 = Use manually configured rules</i> <i>1 = Use configuration files</i>	1	Specifies the way in which IPsec policies are added to the print server.
ipsec_bonjour [Bonjour]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of Bonjour network activities by the IPsec policy.
ipsec_dhcp [DHCP]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of DHCP network activities by the IPsec policy.
ipsec_slp [FTP]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of FTP network activities by the IPsec policy. <u>Note:</u> If all FTP network activities are allowed (FTP = on), you must specify the 'Allow all' action in the default rule.
ipsec_netbios [NetBIOS]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of NetBIOS network activities by the IPsec policy.
ipsec_slp [SLP]	on/off <i>on = activity is always allowed</i> <i>off = activity is filtered via IPsec</i>	off	Enables/disables the filtering of SLP network activities by the IPsec policy.
ipsec_rule1_enabled ~ ipsec_rule4_enabled [Rule 1–4]	on/off	off	Enables/disables the IPsec rules.

Parameters	Value	Default	Description
ipsec_rule1_iaddr_tmpl ~ ipsec_rule4_iaddr_tmpl [Address filter]	0–8 [1 character; 0–8] 0 = --- 1 = Address template 1 2 = Address template 2 3 = Address template 3 4 = Address template 4 5 = Address template 5 6 = Address template 6 7 = Address template 7 8 = Address template 8	0	Specifies the filter within an IPsec rule for the IP traffic via an address template. See parameter 'iaddr_tmpl1_name' ⇨ 185.
ipsec_rule1_iserv_tmpl ~ ipsec_rule4_iserv_tmpl [Service filter]	0–4 [1 character; 0–4] 0 = --- 1 = Service template 1 2 = Service template 2 3 = Service template 3 4 = Service template 4	0	Specifies the filter within an IPsec rule for protocols and services via a service template. See parameter 'iserv_tmpl1_name' ⇨ 185.
ipsec_rule1_action ~ ipsec_rule4_action [Action]	0–2 [1 character; 0–2] 0 = Allow all 1 = Drop all 2 = IPsec require	2	As specified within the IPsec rule, this is the action to be carried out if a data packet matches the description of a filter.
ipsec_rule1_ipsec_tmpl ~ ipsec_rule4_ipsec_tmpl [Security association (SA)]	0–4 [1 character; 0–4] 0 = --- 1 = SA template 1 2 = SA template 2 3 = SA template 3 4 = SA template 4	0	Specifies the parameters of the 'Security Association' via an SA template. See parameter 'ipsec_tmpl1_name' ⇨ 185.

Parameters	Value	Default	Description
ipsec_def_action [Action of the default rule]	0–1 [1 character; 0–1] <i>0 = Allow all</i> <i>1 = Drop all</i>	0	As specified in the IPsec default rule, this is the action to be carried out if a data packet matches the description of a filter.
iaddr_tmpl1_name ~ iaddr_tmpl8_name [Name]	max. 18 characters [a–z, A–Z, 0–9, _, -] <i>iaddr_tmpl1_name = all IP addresses</i> <i>iaddr_tmpl2_name = all IPv4 addresses</i> <i>iaddr_tmpl3_name = all IPv6 addresses</i>	iaddr_tmpl1_name iaddr_tmpl2_name iaddr_tmpl3_name	Name of the address template The template is used for filtering the IP traffic. <i>Local and remote IP addresses can be defined in the address template. Addresses in the format IPv4 and IPv6 are supported.</i>
iaddr_tmpl1_ip_remote ~ iaddr_tmpl8_ip_remote [Remote (IPv4)]	0.0.0.0/0 valid IPv4 address valid IPv4 address range <i>0.0.0.0/0 = all IPv4 addresses</i>	0.0.0.0/0	Specifies a remote IPv4 address or an IPv4 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iaddr_tmpl1_ip6_local ~ iaddr_tmpl8_ip6_local [Local (IPv6)]	:::0 valid IPv6 address valid IPv6 address range <i>:::0 = all IPv6 addresses</i>	:::0	Specifies a local IPv6 address or an IPv6 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iaddr_tmpl1_ip6_remote ~ iaddr_tmpl8_ip6_remote [Remote (IPv6)]	:::0 IPv6 address IPv6 address range <i>:::0 = all IPv6 addresses</i>	:::0	Specifies a remote IPv6 address or an IPv6 address range for an address template. <i>The notation of address ranges is done via the CIDR methodology (e.g. 192.168.0.1/24).</i>
iserv_tmpl1_name ~ iserv_tmpl4_name [Name]	max. 16 characters [a–z, A–Z, 0–9, _, -]	iserv_tmpl1_name = all services	Name of the service template. <i>The template is used for filtering the IP traffic by services and protocols.</i>
ipsec_tmpl1_name ~ ipsec_tmpl4_name [Name]	max. 16 characters [a–z, A–Z, 0–9, _, -]		Name of the SA template. <i>The template specifies the parameters of a 'Security Association'.</i>

Parameters	Value	Default	Description
ipsec_tmpl1_certif icate ~ ipsec_tmpl4_certif icate [Authentication type]	0–1 [1 character; 0-1] <i>0 = pre-shared key</i> <i>1 = certificates</i>	1	Specifies the procedure for the authentication of the remote server.
ipsec_tmpl1_verify ~ ipsec_tmpl4_verify [Verify certificate]	on/off <i>off = self-signed certificate suffices</i> <i>on = CA root certificate is required.</i>	off	Specifies the type of certificate required for the certificate-based authentication.
ipsec_tmpl1_psk ~ ipsec_tmpl4_psk [Pre-Shared Key]	max. 16 characters		Specifies the Pre-Shared Key (PSK). <i>You need the key if the 'Pre-Shared Key' procedure has been selected as 'Authentication type'.</i>
ipsec_tmpl1_key_ exchange ~ ipsec_tmpl4_key_ exchange [IKE]	0–4 [1 character; 0–4] <i>0 = ---</i> <i>1 = IKE template 'IKE Default'</i> <i>2 = IKE template 2</i> <i>3 = IKE template 3</i> <i>4 = IKE template 4</i>	0	Specifies the template to be used for the IKE (automatic key exchange) within a SA. <i>See parameter 'ipsec_key_exchange1_name' → §186.</i> <i>The 'IKE Default' template has been implemented by default. You can specify another 5 templates, if required.</i>
ipsec_key_excha nge1_name ~ ipsec_key_excha nge4_name [Name]	max. 16 characters [a–z, A–Z, 0–9, _, -]	ipsec_ke y_excha nge1_na me = IKE Default	Name of the IKE template

Parameters	Value	Default	Description
ipsec_key_exchange1_modes ~ ipsec_key_exchange4_modes [Negotiation]	main aggressive	main	Specifies the procedure for the negotiation of the encryption and authentication. - In the 'Main Mode' individual connections will be successively established for the individual steps (key exchange, etc.). - In the 'Aggressive Mode' individual steps of the Main Mode will be summarized (faster but less secure). <i>(Both security methods can also be used in combination.) Only the most secure procedure will be applied. If a procedure fails, a less complicated (and therefore less secure) procedure will be used.</i>
ipsec_key_exchange1_dh_group ~ ipsec_key_exchange4_dh_group [Diffie-Hellman group]	1–8 [1 character; 1–8] 1 = modp768 2 = modp1024 3 = modp1536 4 = modp2084 5 = modp3072 6 = modp4096 7 = modp6144 8 = modp8192	2	Specifies the Diffie-Hellman group number for the creation of dynamically generated temporary keys. The keys are used during the negotiation.
ipsec_key_exchange1_encryption_algo_ph1 ~ ipsec_key_exchange4_encryption_algo_ph1 [Encryption algorithm]	0–2 [1 character; 0–2] 0 = DES 1 = 3DES 2 = AES	1	Specifies the encryption algorithm to be used during the negotiation.
ipsec_key_exchange1_hash_algo_ph1 ~ ipsec_key_exchange4_hash_algo_ph1 [Hash algorithm]	0–1 [1 character; 0–1] 0 = MD5 1 = SHA-1	1	Specifies the hash algorithm to be used during the negotiation.

Parameters	Value	Default	Description
ipsec_key_exchange1_lifetime_ph1 ~ ipsec_key_exchange4_lifetime_ph1 [IKE SA lifetime]	600–4294967295 [3 characters; 0–9]		Specifies the duration of the IKE connection in seconds. When the IKE SA lifetime expires, a re-authentication is required.
ipsec_key_exchange1_encapsulation_mode ~ ipsec_key_exchange4_encapsulation_mode [Encapsulation type]	0–1 [1 character; 0–1] <i>0 = transport mode</i> <i>1 = tunnel mode</i>	0	Specifies how the IP data packet is handled within the SA. The IPsec specification differentiates between the 'Transport mode' and the 'Tunnel mode': - In the transport mode the IP data packet is encrypted. However, the IP header will be kept. - In the tunnel mode a complete IP data packet will be encapsulated in another packet and be given a new IP header. Note: The tunnel mode cannot be selected via the selection list on the Print Server Homepage. Use a configuration file (racoon/setkey) instead.
ipsec_key_exchange1_pfs_group ~ ipsec_key_exchange4_pfs_group [Diffie-Hellman group]	0–8 [1 character; 0–8] <i>0 = ---</i> <i>1 = modp768</i> <i>2 = modp1024</i> <i>3 = modp1536</i> <i>4 = modp2084</i> <i>5 = modp3072</i> <i>6 = modp4096</i> <i>7 = modp6144</i> <i>8 = modp8192</i>	ipsec_key_exchange1_pfs_group = 0 ipsec_key_exchange2_pfs_group = 1 ipsec_key_exchange3_pfs_group = 1 ipsec_key_exchange4_pfs_group = 1	Specifies the Diffie-Hellman group number for the creation of additional dynamically generated temporary keys. The keys are used during phase 2.

Parameters	Value	Default	Description
ipsec_key_exchange1_encryption_algorithm_ph2	3des	ipsec_key_exchange1_encryption_algorithm_ph2 = 3des	Specifies the encryption algorithm for phase 2.
~	des	ipsec_key_exchange1_encryption_algorithm_ph2 = des	
ipsec_key_exchange4_encryption_algorithm_ph2	aes	ipsec_key_exchange4_encryption_algorithm_ph2 = aes	<i>You can select several procedures. If the remote party also offers several procedures, the procedure that was listed first with the communication partner will be used.</i>
[Encryption algorithm]	des_iv64	ipsec_key_exchange4_encryption_algorithm_ph2 = des_iv64	
	des_iv32 / null_enc	ipsec_key_exchange4_encryption_algorithm_ph2 = des_iv32	<i>3des = 3DES</i>
	[Multiple algorithms can be defined using a comma-separated list.]	ipsec_key_exchange4_encryption_algorithm_ph2 = des,des_iv32	<i>des = DES</i>
		ipsec_key_exchange4_encryption_algorithm_ph2 = aes	<i>aes = AES</i>
		ipsec_key_exchange4_encryption_algorithm_ph2 = des_iv64	<i>des_iv64 = DES 64</i>
		ipsec_key_exchange4_encryption_algorithm_ph2 = des_iv32	<i>des_iv32 = DES 32</i>
		ipsec_key_exchange4_encryption_algorithm_ph2 = null_enc	<i>null_enc = none</i>

Parameters	Value	Default	Description
ipsec_key_exchange1_auth_algorithm2 ~ ipsec_key_exchange4_auth_algorithm2 [Authentication algorithm]	hmac_md5 hmac_sha1 non_auth [Multiple algorithms can be defined using a comma-separated list.]	ipsec_key_exchange1_auth_algorithm2=hmac_md5,hmac_sha1 ipsec_key_exchange2_auth_algorithm2=hmac_sha1 ipsec_key_exchange3_auth_algorithm2=hmac_sha1 ipsec_key_exchange4_auth_algorithm2=hmac_sha1	Specifies the hash algorithm for phase 2. <i>You can select several procedures. If the remote party also offers several procedures, the procedure that was listed first with the communication partner will be used.</i> <i>hmac_md5 = MD5</i> <i>hmac_sha1 = SHA-1</i> <i>non_auth = none</i>
ipsec_key_exchange1_with_ah ~ ipsec_key_exchange4_with_ah [With AH protocol]	on/off	off	Specifies the use of the 'Authentication Header' protocol for the protection of the packet integrity and packet authentication. <i>AH uses the authentication header to authenticate the packet. In the IP data packet, the authentication header will be added after the IP header.</i>
ipsec_key_exchange1_lifetime_ph2 ~ ipsec_key_exchange4_lifetime_ph2 [IKE SA lifetime]	600–4294967295 [1–10 characters; 0–9]		Defines the time interval in seconds after which the IPsec key of an IPsec SA connection is renewed.

Parameters	Value	Default	Description
iserv_tmpl1_servi ces ~ iserv_tmpl4_servi ces [Services]	ALL ICMP HTTP SNMP SNTP IPP Socket printing LPR ThinPrint	iserv_tm pl1_servi ces = ALL [blank]	Specifies the elements of the service filter. <i>Several protocols can be combined in a service.</i>

Table 42: Parameter List - Dynamic Update

Parameters	Value	Default	Description
dyn_update [Dynamic firmware update]	on/off	off	Enable/disables the dynamic firmware/software update.
dyn_update_url [Update URL]	max. 255 characters	[blank]	Defines the location of the update files needed for the dynamic update.
dyn_proxy [Use proxy server]	on/off	off	Enables/disables the use of a proxy server for the dynamic update.
dyn_proxy_url [Proxy server]	max. 255 characters	[blank]	Defines the URL of the proxy server used for the dynamic update.

Table 43: Parameter List - ThinPrint®

Parameters	Value	Default	Description
tp_port [ThinPrint® port]	1–65535 [1–5 characters; 0–9]	4000	Defines the TCP port used by the print server for communicating with the ThinPrint® server. <i>The port number of the print server must be identical to the port number that was defined on the ThinPrint server.</i>

tp_bandwidth [Bandwidth]	on/off	off	Enables/disables the bandwidth functionality of the ThinPrint® port (print server side).
tp_bandwidthval [Bandwidth]	1600–1000000 [1–7 characters; 0–9]	256000	Defines the bandwidth in bit/second (bit/s) used to decrease the bandwidth limit on the ThinPrint® port (print server side).
lp1_prt_name ~ lp8_prt_name [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer name for the ThinPrint AutoConnect feature.
lp1_prt_class ~ lp8_prt_class [Class]	max. 7 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer class name for the ThinPrint AutoConnect feature.
lp1_prt_driver ~ lp8_prt_driver [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer driver for the ThinPrint AutoConnect feature.

16.3 Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'The print server indicates the BIOS mode' ⇒ 193
- 'Problems With Printing in Windows' ⇒ 194
- 'WLAN configuration fails' ⇒ 195
- 'A connection to the Print Server Homepage cannot be established' ⇒ 195
- 'The password is no longer available' ⇒ 195

Possible Cause

The print server indicates the BIOS mode

The print server switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The print server indicates the BIOS mode if

- the activity LED (yellow) blinks periodically and
- the status LED (green) is not active.



The print server is not operational in the BIOS mode.

If the print server is in the BIOS mode, the filter 'BIOS' will be created automatically in the device list of the InterCon-NetTool. The print server is displayed within this filter.

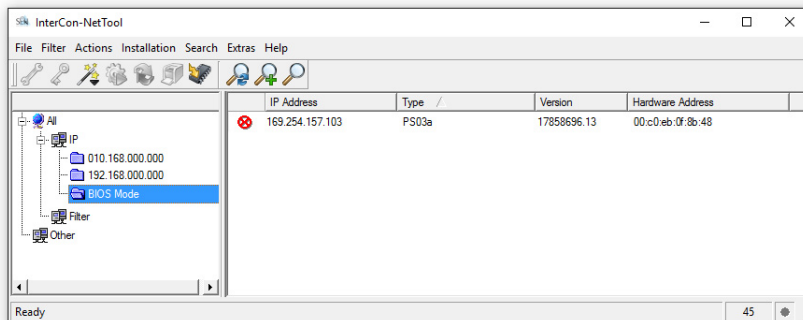




Fig. 10: InterCon-NetTool - print server in the BIOS mode

Requirements

- The InterCon-NetTool is installed on the client, see: ⇒ 15.

 Proceed as follows:

1. *Start the InterCon-NetTool.*
 2. *Select the print server in the device list.*
You will find the print server under the filter 'BIOS mode'.
 3. **Select Installation – IP Wizard.**
The IP Wizard is started.
 4. *Follow the instructions of the wizard in order to assign an IP configuration to the print server.*
The IP configuration is saved.
 5. *Carry out a software update on the print server; see: ⇒ 126.*
-  The software is saved in the print server. The print server switches to the normal mode.

Problems With Printing in Windows

Possible Cause

- GDI (Graphics Device Interface; also known as 'host-based' or 'Windows only') printers use proprietary printer languages. As socket printing only supports standardized printer languages (PCL, PostScript), LPD/LPR printing must be used for GDI printers. Follow the instructions below:
 - Set the communication mode to 'unidirectional' ⇒ 47.

- Configure LPD/LPR printing for the GDI primer ⇒ 16. Make sure to deactivate 'SNMP Status Enabled'.
- Interrupt and re-establish the power supply of the GDI printer ('cold start').

WLAN configuration fails

After you have configured the WLAN parameters, the print server is not displayed in the device list of the InterCon-NetTool.

Possible Cause

Print a status page (⇒ 58) and check if your settings are correct. In the event of incorrect entries, reset the print server parameters (⇒ 122) and repeat the installation; see: Quick Installation Guide.

A connection to the Print Server Homepage cannot be established

Eliminate possible error sources. First of all, check:

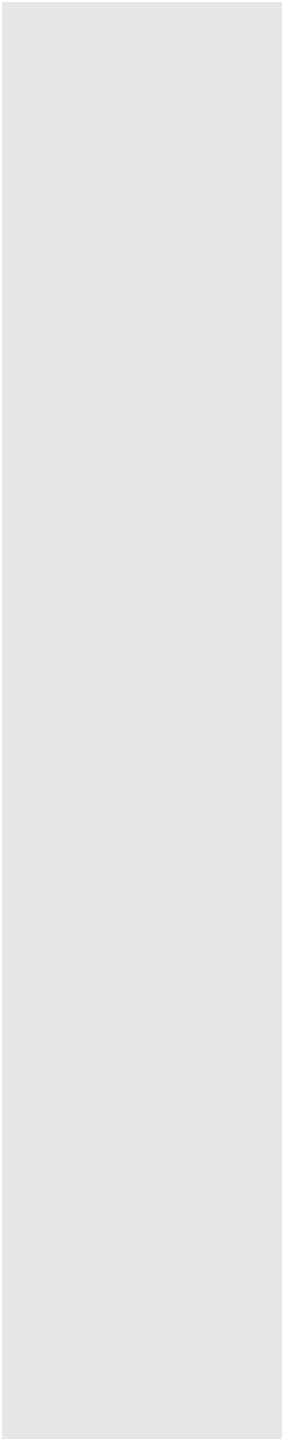
- the cabling connections,
- the print server's IP configuration (⇒ 7), and
- the proxy settings of your browser.

If you still cannot establish any connection, the following safety mechanisms might be the cause:

- 'HTTP' (Hypertext Transfer Protocol) is deactivated. Activate HTTP via the InterCon-NetTool ⇒ 90.
- The access is protected via SSL/TLS (HTTPS) ⇒ 104.
- The access is protected via SSL/TLS (HTTPS) and you deleted the certificate required (CA/self-signed/PKCS#12). Reset the parameter values of the print server to their default settings to get access ⇒ 122. Previous settings will be deleted.
- The password protection is enabled ⇒ 84.

The password is no longer available

The access to the Print Server Homepage can be protected by a password ⇒ 84. If the password is no longer available, you can reset the



parameter values of the print server to their default settings to get access ⇒ 122. Previous settings will be deleted.

16.4 List of Figures

Print server homepage – Home	22
InterCon-NetTool – Main dialog	24
Administration via Email – Example 1	29
Administration via Email – Example 2	30
InterCon-NetTool – IP Wizard	33
InterCon-NetTool – Printer Operating Panel	79
InterCon-NetTool – Parameter download	120
InterCon-NetTool – Standard update	129
IPsec procedure	144
InterCon-NetTool – print server in the BIOS mode	194

16.5 Index

A

- Access control 88
- Ad hoc mode 49
- Address template 149
- Administration methods 20
- ASCII 74
 - Print as PostScript 76
- Authentication 107
- AutoConnect 138

B

- Backup 119
- Bandwidth 137
- Banner page 74
- Baud rate 56
- Bidirectional Communication 54
- Binary PostScript 74
- BIOS mode 193
- Bonjour 41
- Button 125
 - Print service page 66
 - Print status page 66
- Reset 125

C

- CA certificate 93, 94
- Carriage Return with Line Feed (CR+LF) 73
- Certificate 93
- Certification authority 94
- Certification authority (CA) 94
- Channel 50, 170
- Citizen-Z 64
- COM1 55
- Communication mode
 - Bidirectional 54
 - Unidirectional 54
 - WLAN 49
- Configuration parameter. See Parameters

D

- Data bits 56
- Data format 64
- DATAMAX 64
- Default certificate 93
- Default name 161
- Default settings 123
- Description 60
- Device number 161
- DNS 40
- Download
 - Parameters file 25, 119
 - Service page 67
 - Status page 66
- Duplex mode 37
- Dynamic update 128

E

- EAP-FAST 115
- EAP-MD5 108
- EAP-TLS 109
- EAP-TTLS 111
- Email
 - Administration 27
 - Commands 27
 - Notification 81
- Encrypted printing 16
- ESC 72, 74
- Extensible Authentication Protocol (EAP) 107

F

- Factory default settings 123
- Filter Function
 - Find and replace 71
- Filter function 71, 73
 - ASCII/PostScript 72
 - HEX dump mode 72
 - Job Start and Job End 72
 - LF / CR+LF 73
- Filter Settings 73
- Find and Replace 74

- Firmware update 127
 - Flow control 56
 - Frequency range 50
 - FTP 25
 - Configuring parameters 25
 - Print service page 67
 - Print status page 66
 - Update 130
 - FTPS 25
- G**
- Gateway 32, 160
- H**
- Hardware address 62
 - Hex dump mode 73
 - Host name 160
 - Hotline 4
- I**
- IEEE 802.1x 107
 - IEEE1284.4 52
 - IKE template 153
 - Improper Use 5
 - Infrastructure mode 49
 - Intended Use 5
 - InterCon-NetTool 23, 160
 - Installation 23
 - Mode of operation 23
 - Start 23
 - Structure 24
 - Interferences 170
 - Internet Printing Protocol (IPP) 14
 - Printing 14
 - Internet Protocol Security, see IPsec
 - IP address 6, 160
 - IP sender control 90
 - IP-Adresse
 - Saving 6
 - IPsec 141
 - Address template 149
 - Configuration file 155
 - Exceptions 157
 - IKE template 153
 - Policy 141, 157
 - Rule 145, 148
 - SA template 152
 - Security association (SA) 142
 - Service template 151
 - Test mode 157
- IPv6 34
- J**
- Job history 63, 85
- L**
- Language 57
 - LF print as LF+CR 74, 76
 - Line Feed (LF) 73
 - Line Printer Daemon (LPD) 11
 - Logical 161
 - Logical printers 73, 161
- M**
- MIB 43
 - mode 49
- N**
- NetBIOS 38
 - Network Protocols 31
 - Network speed 37
 - Notification
 - Email 81
 - SNMP traps 83
- P**
- Parameter values 123
 - Parameters 162
 - Backup 119
 - Configuration via

- Email 27
 - FTP 25
 - Download 119
 - File 119
 - Reset 123
 - Values 119
 - Parameters file 25
 - Parity 56
 - Password 88
 - PEAP 113
 - PJL 51
 - PKCS#12 94, 102
 - POP3 43
 - Port
 - COM1 55
 - Mode 54
 - Printer 10
 - Settings 51
 - PRESCRIBE 72, 74
 - Print data
 - Conversion 72
 - Modify 71
 - Subsequent editing 71
 - Print Job Language (PJL) 51, 80
 - Print jobs
 - Assignment 69
 - Restrict the acceptance to a certain period of time 68
 - Status 63
 - Timeout 68
 - View 85
 - Print server
 - Description 60
 - Language setting 57
 - Reset 123
 - restart 133
 - Security 87
 - Print server homepage 21
 - Features 21
 - start 21
 - Structure 22
 - Printer
 - Adaptation 73
 - Information 63, 80
 - Port 10
 - Status information 63
 - View Status 78
 - Printer messages
 - E-Mail 81
 - SNMP trap 83
 - Printing
 - Encryption 16
 - Line Printer Daemon (LPD) 11
 - Service page 66, 67
 - Status page 65, 66
 - Printing method
 - Internet Printing Protocol 14
 - Line Printer Daemon (LPD) 11
 - Socket printing
 - 64-bit systems 9
 - Private MIB 43
 - Protection 87
 - Against unauthorized parameter modifications 88
 - Read protection 88
 - Write protection 88
 - Protocol
 - HTTP 89
 - IPv6 34
 - POP3 43
 - SMTP 43
 - SNMP 43
 - SNTP 58
 - TCP/IP 31
 - Public Key 93
- R**
- Read protection 88
 - Remote Authentication Dial-In User Service (RADIUS) 107
 - Requested certificate 94
 - Reset 123
 - Restart 133
 - Roaming 50

S

SA template 152
 Secure printing 16
 Security association 142, 146
 Self-signed certificate 93
 Serial port, see COM1
 Service Page
 Print 64
 Service page 64
 Data format 64
 Download 67
 Mode 64
 Service template 151
 Signature 93
 SMTP 43
 SNMP 43
 Traps 83
 SNTP server 58
 Socket 161
 Socket printing 9
 64-bit systems 9
 Software update 127
 SSID (Service Set Identifier) 50,
 170
 Standard update 127
 Status
 Bonjour 63
 General 62
 IPsec 63
 IPv6 63
 Job history 63
 Mail 63
 POP3 63
 Print server 62
 Printer 78
 Printer port 63
 SMTP 63
 WLAN 62
 Status page 64
 Data format 64
 Download 66
 Mode 64
 Print 64
 Stop bits 56

Subnet mask 32, 161
 Support 4

T

TCP/IP 31
 Test mode 157
 ThinPrint
 Client 135
 Engine 135
 ThinPrint® 135
 AutoConnect 138
 Bandwidth 137
 Port 136
 Printer class 138
 SSL/TLS encryption 140
 Time of the device 58
 Time server 58
 Time stamp 58
 Time zone 58
 Timeout 68

U

Unidirectional communication 54
 Update 127
 automatic 128
 dynamic 127
 Several print servers 132
 standard 127
 via Email 27
 via FTP 132
 UTC 58

V

Version number 62
 Viruses 89

W

WEP 48
 WINS 38
 WLAN 47
 WPA/WPA2 48

Write protection 88

